symantec™

Norton AntiVirus™ 2003 Professional Edition

User's Guide

Norton AntiVirus™ Professional Edition User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 9.0

PN: 10023613

Copyright Notice

Copyright © 2002 Symantec Corporation

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Norton SystemWorks, LiveUpdate, Norton AntiVirus, and Norton Utilities are U.S. registered trademarks of Symantec Corporation. Rescue Disk and Symantec AntiVirus are trademarks of Symantec Corporation.

Microsoft, MSN, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Prodigy Internet is a trademark of Prodigy. Pentium is a registered trademark of Intel Corporation.Yahoo! is a registered trademark of Yahoo! Inc. Palm OS is a registered trademark of Palm, Inc.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT

NORTON ANTIVIRUS PROFESSIONAL EDITION

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. LICENSE:

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use one copy of the Software on each of two (2) single computers. If a License Module accompanies, precedes, or follows this license, You may make that number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network; and

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which You have purchased a subscription for Content Updates for the Software (including any subscription included with Your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. SIXTY (60) DAY MONEY BACK GUARANTEE:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service, for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

4. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL

PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

6. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

7. EXPORT REGULATION:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

8. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

If you're installing Norton AntiVirus Professional Edition for the first time

Start here

Determine which file system your computer uses.

1 **On your desktop, double-click My Computer, right-click drive C, then click Properties.**

? **Which file system are you using?**

- FAT (Windows 98/Me/2000/XP)
  See "If you use a FAT file system" on page 6.
- NTFS (Windows 2000/XP only)
  See "If you use an NTFS file system" on page 7.

For detailed instructions and an animated Web tutorial that walks you through each step of the process, go to www.service.symantec.com/installtutorial

If you use a FAT file system

Check for viruses that affect installation.

1 **Insert the Norton AntiVirus Professional Edition CD into your CD-ROM drive and restart your computer.**

If you do not have a Norton AntiVirus Professional Edition CD or cannot start your computer from a CD, create Emergency Disks on another uninfected computer.

See "Create Emergency Disks" on page 26.

2 **Run a full system scan.**

? **Was a virus found?**

- Yes
  Run a virus scan again using the Delete switch.
- No
  See "Finish installation" on page 8.

For detailed instructions and an animated Web tutorial that walks you through each step of the process, go to www.service.symantec.com/installtutorial

If you use an NTFS file system

Check for viruses that affect installation.

Can you establish a connection to the Internet?

- **Yes**
  Go to http://security.symantec.com and follow the on-screen instructions to scan for threats.
- No
  For Windows XP: Go to service.symantec.com
  For WIndows 2000: Go to service.symantec.com

  See "Finish installation" on page 8.

Was a virus found?

- Yes
  Write down the name of the virus and go to http://securityresponse.symantec.com to locate specific removal instructions.
- No
  If you have not already done so, install Norton AntiVirus Professional Edition.

  See "Finish installation" on page 8.

For detailed instructions and an animated Web tutorial that walks you through each step of the process, go to www.service.symantec.com/installtutorial

Finish installation

After you've checked for viruses, it's safe to install Norton AntiVirus Professional Edition.

1. **Uninstall any other antivirus programs on your computer.**

   On your desktop, use the Add/Remove Programs Control Panel to select the program to uninstall.

2. **Close all open programs on your computer including the items running in the Windows system tray.**

3. **Install Norton AntiVirus Professional Edition from the Norton AntiVirus Professional Edition CD.**
   See "Install Norton AntiVirus Professional Edition" on page 27.

? **Did you see the message "Norton AntiVirus has been installed successfully"?**

- Yes
  See "After installation" on page 31.
- No
  Write down the error message on the screen and go to http://service.symantec.com for further assistance.

Contents

If you're installing Norton AntiVirus Professional Edition for the first time

Start here 5
If you use a FAT file system 6
If you use an NTFS file system 7
Finish installation 8

Chapter 1 About Norton AntiVirus Professional Edition

What's new in Norton AntiVirus Professional Edition 15
How viruses work 16
- Macro viruses spread quickly 17
- Trojan horses hide their true purposes 17
- Worms take up space 17
- How viruses spread 17

How Norton AntiVirus Professional Edition works 18
- The virus definition service stops known viruses 18
- Bloodhound technology stops unknown viruses 19
- Script Blocking stops script-based viruses 19
- Worm Blocking stops worms before they spread 19
- Auto-Protect keeps you safe 20
- UnErase recovers lost or missing files 20
- Wipe Info permanently deletes files 20

How to maintain protection 20
- Avoid viruses 21
- Prepare for emergencies 22

Chapter 2 Installing Norton AntiVirus Professional Edition

System requirements 23
Email clients 24
Supported instant messenger clients 25
Before installation 25
If you suspect that you have a virus 25
Prepare your computer 25
Create Emergency Disks 26
Install Norton AntiVirus Professional Edition 27
If the opening screen does not appear 31
After installation 31
Restart your computer 32
Use the Information Wizard 32
Read the Readme file 34
If you need to uninstall Norton AntiVirus Professional Edition 35

Chapter 3 Norton AntiVirus Professional Edition basics

Access Norton AntiVirus Professional Edition tools 37
Use the Norton AntiVirus Professional Edition main window 37
Use the Windows Explorer toolbar 38
Use the Norton AntiVirus Windows tray icon 39
Check the version number 39
Temporarily disable Auto-Protect 39
Maintain Norton AntiVirus Professional Edition protection 40
About Rescue Disks 40
Create a Rescue Disk set 41
Test your Rescue Disks 41
Update your Rescue Disks 42
Check system status 42
Check Office Plug-in status 44
Customize Norton AntiVirus Professional Edition 44
About System options 45
About Internet options 47
About Other options 48
Change Norton AntiVirus Professional Edition options 48
If you need to restore default settings in Options 49
Password protect Norton AntiVirus options 50
Monitoring Norton AntiVirus Professional Edition activities 50

For more information 51
Look up glossary terms 51
Use online Help 52
Use the User's Guide PDF 53
About Norton AntiVirus Professional Edition on the Web 54
Explore online tutorials 55
Subscribe to the Symantec Security Response newsletter 56

Chapter 4 Protecting disks, files, and data from viruses
Ensure that protection settings are enabled 57
Manually scan disks, folders, and files 58
Perform a full system scan 59
Scan individual elements 59
If problems are found during a scan 60
Create and use custom scans 60
Run a custom scan 61
Delete a custom scan 62
Schedule scans 62
Schedule a custom scan 62
Edit scheduled scans 64
Delete a scan schedule 64

Chapter 5 Keeping current with LiveUpdate
About program updates 65
About protection updates 66
About your subscription 66
When you should update 67
Request an update alert 67
If you run LiveUpdate on an internal network 67
If you can't use LiveUpdate 68
Obtain updates using LiveUpdate 68
Set LiveUpdate to Interactive or Express mode 68
Turn off Express mode 69
Run LiveUpdate automatically 70

Chapter 6 What to do if a virus is found
If a virus is found during a scan 73
Review the repair details 74
Use the Repair Wizard 74
If a virus is found by Auto-Protect 75
If you are using Windows 98/98SE/Me 75
If you are using Windows 2000/XP 76
If a virus is found by Script Blocking 77
If a threat is found by Worm Blocking 77
If Inoculation alerts you about a change in system files 78
If you have files in Quarantine 78
If Norton AntiVirus cannot repair a file 80
If your computer does not start properly 80
If you need to use Rescue Disks (Windows 98/98SE/Me) 80
If you need to use Emergency Disks 81
Look up viruses on the Symantec Web site 82
Look up viruses in Norton AntiVirus 83

Chapter 7 Recovering missing or erased files
About Norton Protection 85
About UnErase Wizard 86
Recover a file with UnErase Wizard 87

Chapter 8 Eliminating data permanently
About Wipe Info 89
About hexadecimal values 90
About the Government Wipe process 90
Set Wipe Info options 91
Wipe files or folders 92

Chapter 9 Troubleshooting

Explore the Symantec service and support Web site 93
Troubleshoot Norton AntiVirus Professional Edition problems 95
My Rescue Disk does not work 95
The alert tells me to use my Rescue Disks, but I did not create them 95
I cannot start from drive A 96
Auto-Protect does not load when I start my computer 97
I have scanned and removed a virus, but it keeps infecting my files 98
Norton AntiVirus Professional Edition cannot repair my infected files 98
I get an error when testing basic Rescue Disks 99
I can't receive email messages 99
I can't send email messages 100

Service and support solutions

Glossary

Index

CD Replacement Form

About Norton AntiVirus Professional Edition

1

Norton AntiVirus Professional Edition provides essential computer protection for small businesses and professionals. This powerful antivirus product safeguards your computer from viruses, helps you recover lost or deleted files, and lets you completely erase confidential files.

Norton AntiVirus Professional Edition provides comprehensive *virus* prevention, detection, and elimination software for your computer. It automatically finds and repairs *infected file*s to keep your data safe and secure. Easy updating of the *virus definition* service over the Internet keeps Norton AntiVirus Professional Edition prepared for the latest threats. Worm Blocking and Script Blocking detect new threats before virus definitions are created.

Advanced tools in Norton AntiVirus Professional Edition help you securely recover lost, deleted, or overwritten files and permanently remove unwanted files that result from a virus or threat to your computer.

What's new in Norton AntiVirus Professional Edition

Norton AntiVirus 2003 Professional Edition expands file repair and deletion options and introduces virus protection for instant messenger attachments, Worm Blocking, password protection for Norton AntiVirus options, and the Log Viewer with more detailed visibility into protection activities.

The new features are:

- Expanded file repair and deletion
  Norton AntiVirus Professional Edition now automatically repairs all repairable files without any interaction with you. Additionally, when Norton AntiVirus finds a worm or Trojan horse, it automatically deletes the infected file(s).
- Instant messenger support and options
  Norton AntiVirus Professional Edition now scans files received by America Online, Yahoo!, and MSN instant messenger programs. You can choose to scan files received by one or all three programs. Norton AntiVirus Professional Edition automatically repairs or *quarantines* the infected file(s).
- Worm Blocking
  Norton AntiVirus Professional Edition scans outgoing email attachments for worms and alerts you before sending any *infected files*. Norton AntiVirus blocks the worm and recommends the appropriate action, so you prevent sending it in an email message.
- Password protection
  Norton AntiVirus Professional Edition allows you to set, change, and reset a password to control your option settings, so that unauthorized users can't tamper with your virus protection.
- Log Viewer
  Norton AntiVirus Professional Edition organizes information about virus alerts, application activities, and errors. You determine how many activities you want to record.

How viruses work

A software *virus* is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files and, when activated, may damage files, cause erratic system behavior, or display messages.

Computer viruses infect system files and documents created by programs with macro capabilities. Some system viruses are programmed specifically to corrupt programs, delete files, or erase your disk.

Macro viruses spread quickly

Macros are simple programs that are used to do things such as automate repetitive tasks in a document or make calculations in a spreadsheet. Macros are written in files created by such programs as Microsoft Word and Microsoft Excel.

Macro viruses are malicious macro programs that are designed to replicate themselves from file to file and can often destroy or change data. Macro viruses can be transferred across platforms and spread whenever you open an *infected file*.

Trojan horses hide their true purposes

Trojan horses are programs that appear to serve some useful purpose or provide entertainment, which encourages you to run them. But the programs also serve a covert purpose, which may be to damage files or place a virus on your computer.

A Trojan horse is not a virus because it does not replicate and spread like a virus. Because Trojan horses are not viruses, files that contain them cannot be repaired. To ensure the safety of your computer, Norton AntiVirus Professional Edition detects Trojan horses so you can delete them from your computer.

Worms take up space

Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk. They search for specific types of files and try to damage or destroy those files. Worms replicate only in memory, creating myriad copies of themselves, all running simultaneously, which slows down the computer. Other worms spread through your email address list and can email themselves without you knowing. Like Trojan horses, worms are not viruses and therefore cannot be repaired. They must be deleted from your computer.

How viruses spread

A virus is inactive until you launch an infected program, start your computer from a disk that has infected system files, or open an infected document. For example, if a word processing program contains a virus, the virus activates when you run the program. Once a virus is in memory, it usually infects any program you run, including *network* programs (if you can make changes to network folders or disks).

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected program is running. Turning off your computer or exiting the program removes the virus from memory, but does not remove the virus from the infected file or disk. That is, if the virus resides in an operating system file, the virus activates the next time you start your computer from the infected disk. If the virus resides in a program, the virus activates the next time you run the program.

To prevent virus-infected programs from getting onto your computer, Norton AntiVirus Professional Edition automatically scans files before you copy or run them. This includes programs you *download* from news groups or Internet Web sites and any email attachments that you receive.

Viruses spread through email and instant messenger attachments. Norton AntiVirus monitors incoming and outgoing email messages and instant messenger attachments for potential *threats.*

How Norton AntiVirus Professional Edition works

Norton AntiVirus Professional Edition monitors your computer for known and unknown viruses. A *known virus* is one that can be detected and identified by name. An *unknown virus* is one for which Norton AntiVirus Professional Edition does not yet have a definition.

Norton AntiVirus Professional Edition continually monitors your computer to protect you from both types of viruses, using virus definitions to detect known viruses, and Bloodhound technology, Script Blocking, and Worm Blocking to detect unknown viruses. Virus definitions, Bloodhound technology, Script Blocking, and email and instant messenger scanning are all used during scheduled scans and manual scans, and are used by Auto-Protect to constantly monitor your computer.

The virus definition service stops known viruses

See "Look up viruses in Norton AntiVirus" on page 83.

The virus definition service consists of files that Norton AntiVirus Professional Edition uses to recognize viruses and intercept their activity. You can look up virus names in Norton AntiVirus Professional Edition, and access an encyclopedia of virus descriptions on the Symantec Web site.

Bloodhound technology stops unknown viruses

Bloodhound is the Norton AntiVirus Professional Edition scanning technology for detecting new and unknown viruses. It detects viruses by analyzing a file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data contained in the file. It also sets up simulated environments in which to load documents and test for macro viruses.

Script Blocking stops script-based viruses

A script is a program written with a scripting language, such as Visual Basic Script or JavaScript and can be executed without user interaction. Scripts can be opened with text editors or word processing programs, so they are very easy to change.

Scripts can be used when you log on to the Internet, or check your email. Restarting your computer involves using scripts that tell your computer what programs to load and run.

A script can also be written to perform malicious activities when it is launched. You can unknowingly receive a malicious script by opening an infected document or email attachment, viewing an infected *HTML* email message, or visiting an infected Internet Web site.

Script Blocking detects Visual Basic and JavaScript viruses without the need for specific virus definitions. It monitors the scripts for *virus-like activity* and alerts you if it is found.

Worm Blocking stops worms before they spread

Worms hide in files and are not active or dangerous until the files are opened. You can unknowingly copy or send an infected file by email. A file infected with a worm cannot be repaired; it must be deleted.

Worm Blocking scans all outgoing email messages and alerts you if a malicious worm is detected. Once a worm is detected, Norton AntiVirus blocks the worm and recommends the appropriate action, so you prevent sending it in an email message.

Auto-Protect keeps you safe

Norton AntiVirus Professional Edition Auto-Protect loads into memory when Windows starts, providing constant protection while you work.

Using Auto-Protect, Norton AntiVirus Professional Edition automatically:

- Eliminates viruses, worms, and Trojan horses, including macro viruses, and repairs damaged files
- Checks for viruses every time you use software programs on your computer, insert floppy disks or other removable media, or use document files that you receive or create
- Monitors your computer for any unusual symptoms that may indicate an active virus
- Protects your computer from Internet-borne viruses

UnErase recovers lost or missing files

UnErase helps you recover deleted files that are moved to the Norton Protected Recycle Bin. The Norton Protected Recycle Bin enhances the Windows Recycle Bin by protecting files from permanent deletion. UnErase Wizard lets you recover these protected files.

Wipe Info permanently deletes files

Wipe Info permanently wipes or erases the contents of a file to protect your sensitive information. Wipe Info can wipe a specific file or entire folders and provides a Fast Wipe or a Government Wipe for ultimate security.

How to maintain protection

When Norton AntiVirus Professional Edition is installed, you have complete virus protection. However, new viruses are created constantly. Viruses can spread when you start your computer from an infected disk or run an infected program. There are several things you can do to avoid viruses and to recover quickly should a virus strike.

Avoid viruses

It is important that you practice regular file maintenance and keep Norton AntiVirus Professional Edition up-to-date.

To avoid viruses:

- Write-protect removable media.
- Stay informed about viruses by logging on to the Symantec Security Response Web site (http://securityresponse.symantec.com) where there is extensive, frequently updated information on viruses and virus protection.

See "About Norton AntiVirus Professional Edition on the Web" on page 54.

- Keep LiveUpdate turned on at all times to continually update your virus definitions files.

See "Keeping current with LiveUpdate" on page 65.

- Run LiveUpdate regularly to receive new program updates.
- Keep Norton AntiVirus Professional Edition Auto-Protect turned on at all times to prevent viruses from infecting your computer.
- If Norton AntiVirus Professional Edition Auto-Protect is not turned on, scan removable media before you use them.

See "Manually scan disks, folders, and files" on page 58.

- Schedule periodic scans to occur automatically.

See "Schedule scans" on page 62.

- Watch for *email* from unknown senders. Do not open anonymous attachments.
- Keep Worm Blocking turned on to avoid sending infected email attachments.
- Keep Script Blocking turned on to detect any virus-like activity.
- Keep all recommended maximum protection settings turned on.

See "Ensure that protection settings are enabled" on page 57.

Prepare for emergencies

It is also important that you are prepared in case your computer is infected by a virus.

To prepare for emergencies:

- Back up files regularly and keep more than just the most recent backup.
- If you are using a computer that cannot start from a CD, create a set of Emergency Disks, from which you can start your computer and scan for viruses.

See "Create Emergency Disks" on page 26.

- If you are using Windows 98 or Me, create and keep updated a set of Rescue Disks, with which you can start your computer in DOS mode and use Norton AntiVirus Professional Edition to fix virus-related problems and recover from a system crash.

See "About Rescue Disks" on page 40.

Installing Norton AntiVirus Professional Edition

2

Before installing Norton AntiVirus Professional Edition, take a moment to review the system requirements listed in this chapter. Windows 98/Me users should have several blank 1.44-MB disks available to make Rescue Disks.

System requirements

To use Norton AntiVirus Professional Edition, your computer must have one of the following Windows *operating systems*:

- Windows 98/98SE/Me
- Windows 2000 Professional Edition
- Windows XP Professional/Home Edition

Installation of Norton AntiVirus Professional Edition is not supported on Windows 95/NT, Macintosh, Linux, or server versions of Windows 2000/XP computers.

If you are planning to upgrade your Windows operating system from Windows 98/Me to Windows 2000/XP, you must uninstall Norton AntiVirus Professional Edition first and then reinstall after the upgrade is complete.

Your computer must also meet the following minimum requirements.

Operating system	Requirements
Windows 98/Me	■ Intel Pentium processor (or compatible) at 133 MHz for Windows 98; 150 MHz for Windows Me ■ 32 MB of RAM ■ 70 MB of available hard disk space ■ Internet Explorer 5.0 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows 2000 Professional Edition	■ Intel Pentium processor (or compatible) at 133 MHz or higher ■ 64 MB of RAM ■ 70 MB of hard disk space ■ Internet Explorer 5.0 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive
Windows XP Professional/Home Edition	■ Intel Pentium processor (or compatible) at 300 MHz or higher ■ 128 MB of RAM ■ 70 MB of hard disk space ■ Internet Explorer 5.0 or later (5.5 recommended) ■ CD-ROM or DVD-ROM drive

If you are installing on Windows 2000/XP, you must install with administrator privileges.

Email clients

Email scanning is supported for any POP3 compatible email client including:

- Microsoft Outlook Express version 4, 5 or 6
- Microsoft Outlook 97/98/2000/XP
- Netscape Messenger version 4, Netscape Mail version 6
- Eudora Light version 3, Eudora Pro version 4, Eudora version 5
- Pegasus 4

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- POP3s with SSL (Secure Sockets Layer)
- Web-based email such as Hotmail and Yahoo!
- Lotus Notes mail

Supported instant messenger clients

- AOL Instant Messenger, version 4.7 or later
- Yahoo! Instant Messenger, version 5.0 or later
- MSN Messenger and Windows Messenger, version 4.6 or later

Before installation

See "Create Emergency Disks" on page 26.

Before you install Norton AntiVirus Professional Edition, prepare your computer. If your computer cannot start from a CD, create Emergency Disks.

If you suspect that you have a virus

See "Start here" on page 5.

If you try to install and your computer has a virus, Norton AntiVirus Professional Edition requests that you restart your computer. Restart from the Norton AntiVirus Professional Edition CD and scan your computer's hard disk for viruses. The Norton AntiVirus emergency program uses the virus definitions from the Norton AntiVirus Professional Edition CD, and is not as up-to-date as virus definitions downloaded using LiveUpdate.

Once the virus has been repaired, delete the Norton AntiVirus Professional Edition install files in the temporary folder that are left behind after the forced shutdown.

Prepare your computer

See "If you need to uninstall Norton AntiVirus Professional Edition" on page 35.

If you have version 2000-2002 of Norton AntiVirus Professional Edition, the new version automatically removes the older version. If your version is older than 2000, you must uninstall it before installing the new version. If you have Norton AntiVirus 2002 Professional Edition, you can transfer your existing option settings to the new version of the program.

Norton AntiVirus 2003 Professional Edition does not include Symantec AntiVirus for Palm OS. If you have Norton AntiVirus 2002 or 2001 Professional Edition, you are able to keep your version of Symantec AntiVirus for Palm OS when installing Norton AntiVirus 2003 Professional Edition, if you choose.

Before you install Norton AntiVirus, use these suggestions to prepare your computer:

- If you have any other antivirus programs on your computer, you must uninstall them and restart your computer before installing Norton AntiVirus Professional Edition.
  To uninstall other antivirus programs, see the user documentation that came with the program.
- Close all other Windows programs before installing Norton AntiVirus Professional Edition, including those programs displayed in the Windows tray.

Create Emergency Disks

"If you need to use Emergency Disks" on page 81.

Emergency Disks are used to start your computer and scan for viruses in case of a problem. If your computer can start from a CD, you can use the Norton AntiVirus Professional Edition CD in place of Emergency Disks and do not need to create them.

If you cannot start your computer, you can use these instructions to create Emergency Disks on another computer or go to http://www.symantec.com/techsupp/ebd.html and download the Emergency Disk program. Follow the instructions included in the download to create the Emergency Disks.

You will need several formatted 1.44 MB disks.

To create Emergency Disks

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Support** folder.
4. Double-click the **Edisk** folder.
5. Double-click **NED.exe**.
6. In the welcome window, click **OK**.
7. Label the first disk as instructed and insert it into drive A.
8. Click **Yes**.
9. Repeat steps 7 and 8 for the subsequent disks.
10. When the procedure is complete, click **OK**.
11. Remove the final disk from drive A and store the Emergency Disk set in a safe place.

Install Norton AntiVirus Professional Edition

Install Norton AntiVirus Professional Edition from the Norton AntiVirus Professional Edition CD.

To install Norton AntiVirus Professional Edition

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.

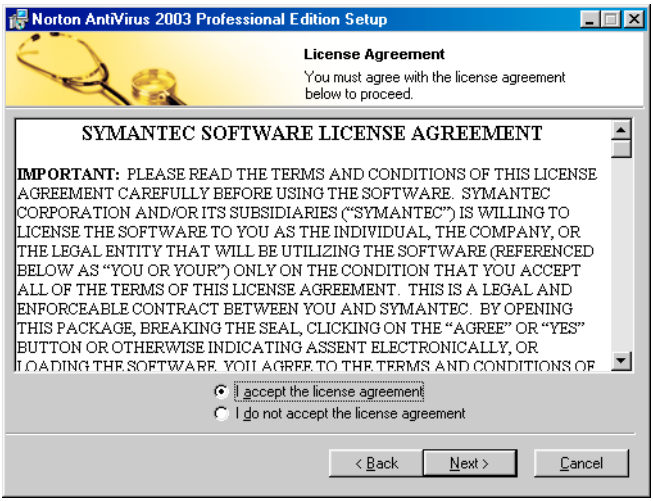
See "If the opening screen does not appear" on page 31.

2. In the Norton AntiVirus Professional Edition window, click **Install Norton AntiVirus Professional Edition**.
   If your computer is not set to automatically open a CD, you will have to open it yourself.

See "Test your Rescue Disks" on page 41.

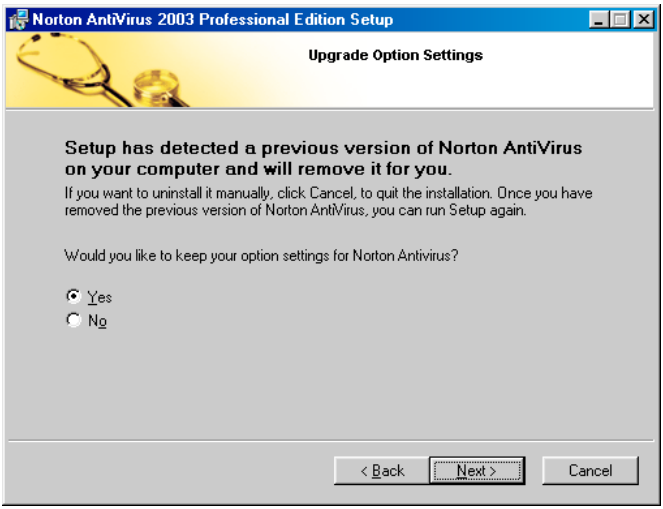
3. If you are installing in Windows 98/98SE/Me, Norton AntiVirus scans your computer's memory for viruses before installing. If a virus is found, you are prompted to use your Emergency Disks to remove the virus before continuing.
4. The opening installation window reminds you to close all other Windows programs.

5 Click **Next**.


Norton AntiVirus 2003 Professional Edition Setup
License Agreement
You must agree with the license agreement below to proceed.
SYMANTEC SOFTWARE LICENSE AGREEMENT
IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR
I accept the license agreement
I do not accept the license agreement
< Back
Next >
Cancel

6 Read the License Agreement and click **I accept the license agreement**.
If you decline, you cannot continue with the installation.

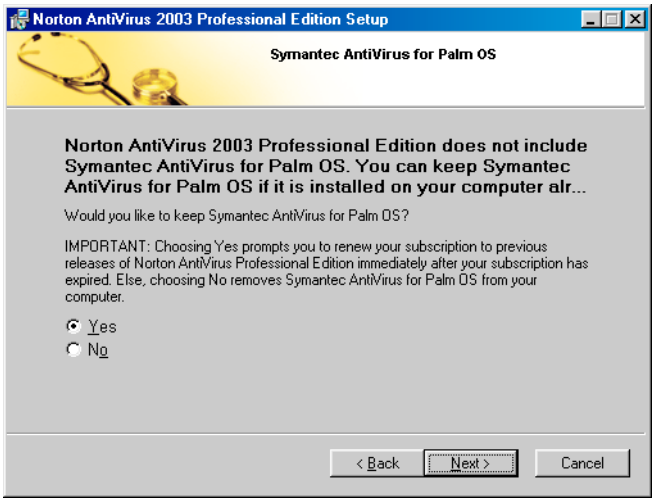
7 Click **Next**.


Norton AntiVirus 2003 Professional Edition Setup
Upgrade Option Settings
Setup has detected a previous version of Norton AntiVirus on your computer and will remove it for you.
If you want to uninstall it manually, click Cancel, to quit the installation. Once you have removed the previous version of Norton AntiVirus, you can run Setup again.
Would you like to keep your option settings for Norton Antivirus?
Yes
No
< Back
Next >
Cancel

See "Prepare your computer" on page 25.

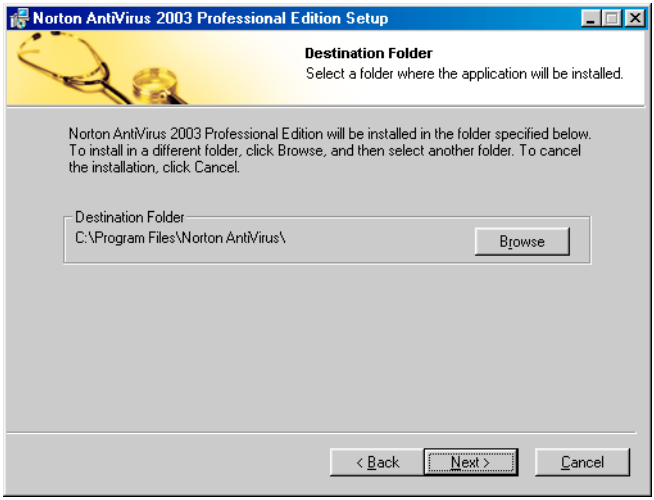
8 If you have version 2002 of Norton AntiVirus or Norton AntiVirus Professional Edition installed on your computer, you can keep your option settings. Click **Yes** to keep the settings.

9 Click **Next**.


Norton AntiVirus 2003 Professional Edition Setup
Symantec AntiVirus for Palm OS
Norton AntiVirus 2003 Professional Edition does not include Symantec AntiVirus for Palm OS. You can keep Symantec AntiVirus for Palm OS if it is installed on your computer alr...
Would you like to keep Symantec AntiVirus for Palm OS?
IMPORTANT: Choosing Yes prompts you to renew your subscription to previous releases of Norton AntiVirus Professional Edition immediately after your subscription has expired. Else, choosing No removes Symantec AntiVirus for Palm OS from your computer.
Yes
No
< Back
Next >
Cancel

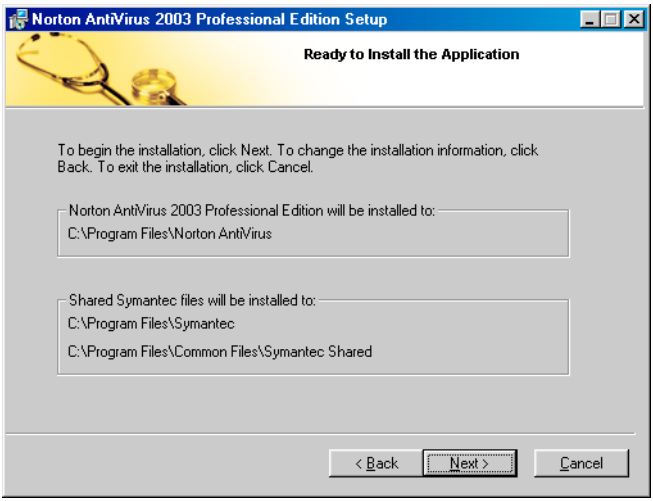
10 If you have Norton AntiVirus 2001 or 2002 Professional Edition installed on your computer, you can keep the Symantec AntiVirus for Palm OS component installed. Click **Yes** to keep the component installed.

11 Click **Next**.

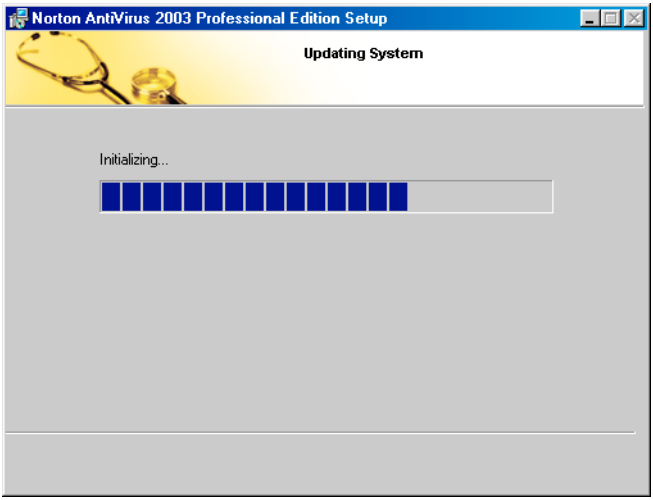

Norton AntiVirus 2003 Professional Edition Setup
Destination Folder
Select a folder where the application will be installed.
Norton AntiVirus 2003 Professional Edition will be installed in the folder specified below. To install in a different folder, click Browse, and then select another folder. To cancel the installation, click Cancel.
Destination Folder
C:\Program Files\Norton AntiVirus\
Browse
< Back
Next >
Cancel

12 Click **Browse** to select a folder into which you want to install Norton AntiVirus Professional Edition.

13 Click **Next**.

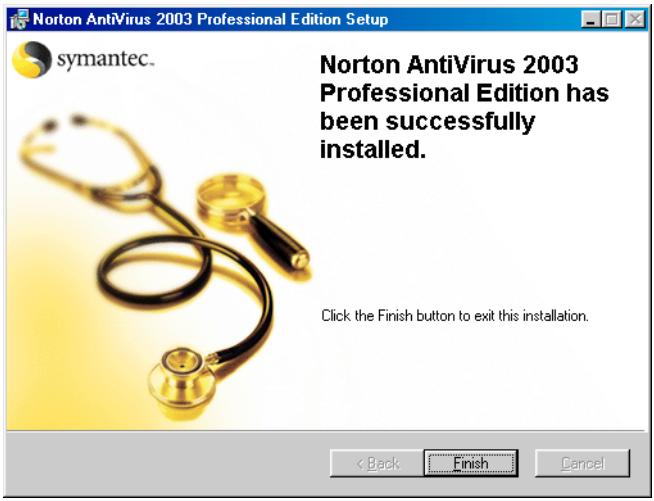

Norton AntiVirus 2003 Professional Edition Setup
Ready to Install the Application
To begin the installation, click Next. To change the installation information, click Back. To exit the installation, click Cancel.
Norton AntiVirus 2003 Professional Edition will be installed to:
C:\Program Files\Norton AntiVirus
Shared Symantec files will be installed to:
C:\Program Files\Symantec
C:\Program Files\Common Files\Symantec Shared
< Back
Next >
Cancel

14 Confirm the installation location, then click **Next**.



See "Read the Readme file" on page 34.

15 After Norton AntiVirus is installed, scroll through the Readme text, then click **Next**.


Norton AntiVirus 2003 Professional Edition Setup
symantec.
Norton AntiVirus 2003 Professional Edition has been successfully installed.
Click the Finish button to exit this installation.
< Back
Finish
Cancel

16 Click **Finish** to exit the installation.

If the opening screen does not appear

Sometimes, a computer's CD-ROM drive does not automatically start a CD.

To start the installation from the Norton AntiVirus Professional Edition CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer dialog box, double-click the icon for your CD-ROM drive.

3 From the list of files, double-click **CDSTART.EXE**.

After installation

For Windows 98/Me, you must restart your computer after installing Norton AntiVirus Professional Edition.

If your computer needs to be restarted after Norton AntiVirus Professional Edition is installed, a prompt appears giving you the option to do so immediately. After restart or, if your computer does not need to be restarted, after installation is complete, the Information Wizard appears.

Restart your computer

After installation, you may receive a prompt telling you that your computer needs to be restarted in order for the updates to take effect.

To restart your computer

- In the dialog box, click **Yes**.
  If you click No, configuration of Norton AntiVirus Professional Edition is not complete until you restart your computer.

Use the Information Wizard

The Information Wizard lets you register your copy of Norton AntiVirus Professional Edition, get information about the virus definition subscription service, select post-install tasks to be done automatically, and review your Norton AntiVirus Professional Edition settings.

If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register on the Symantec Web site at www.symantec.com or by using the Product Registration option on the Help menu. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

1. In the welcome window, click **Next**.
2. In the first Registration window, select the country/Region from which you are registering and the country/Region in which you live (if different), then click **Next**.
3. If you would like information from Symantec about Norton AntiVirus Professional Edition, select the method by which you want to receive that information, then click **Next**.
4. Enter your name and whether you want Norton AntiVirus Professional Edition registered to you or your company, then click **Next**.
5. Enter your address, then click **Next**.
6. Answer the survey questions to help Symantec improve its products and services, then click **Next** when you are done or to skip the survey.
7. Select whether you want to register Norton AntiVirus Professional Edition through the Internet or by mail, then click **Next**.
   If you submitted your registration through the Internet, a dialog box displays the serial number for your product.

8 Write down the number or click **Print** to get a copy of your registration information for future reference.

9 Click **Next**.

10 Select whether you want to use your existing profile the next time you register a Symantec product, or type the information as part of registration.

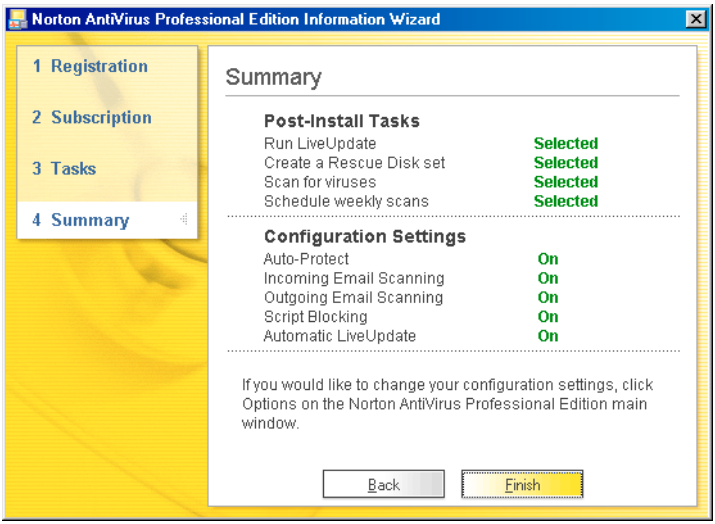
11 Click **Finish**.

12 Review the subscription service information, then click **Next**.

13 Select the post-install tasks that you want Norton AntiVirus Professional Edition to perform automatically. Your options are:

Run LiveUpdate to ensure that you have the latest virus definitions.	See "Keeping current with LiveUpdate" on page 65.
If you are installing in Windows 98/Me, you also have the option to create a Rescue Disk set.	See "About Rescue Disks" on page 40.
Perform a full system scan.	See "Manually scan disks, folders, and files" on page 58.
Schedule a weekly scan of your local hard drives. You must have Microsoft Scheduler installed to use this option. If you select this option, you can change the schedule for this scan as desired.	See "Schedule scans" on page 62.

14 Click **Next**.



See "Customize Norton AntiVirus Professional Edition" on page 44.

15 Review the configuration settings for Norton AntiVirus Professional Edition. If you want to change any of the settings, do so using Options.

16 Click **Finish**.

If you selected any post-install tasks, they start automatically.

Read the Readme file

The Readme file contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the Norton AntiVirus Professional Edition product files.

To read the Readme file

1 Using Windows Explorer, navigate to the location where your Norton AntiVirus Professional Edition files are installed.
If you installed Norton AntiVirus Professional Edition in the default location, the files are in C:\Program Files\Norton AntiVirus.

2 Double-click **Readme.txt** to open the file in Notepad or WordPad.
The Readme file includes instructions for printing it if you want to do so.

3 Close the word processing program when you are done reading the file.

If you need to uninstall Norton AntiVirus Professional Edition

If you need to remove Norton AntiVirus Professional Edition from your computer, use the Add/Remove Programs option from the Windows Control Panel or the Uninstall Norton AntiVirus Professional Edition option from the Programs menu.

During uninstall, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

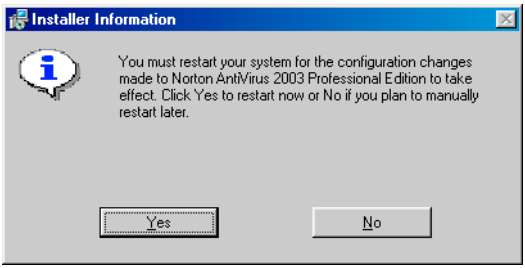
To uninstall Norton AntiVirus Professional Edition

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton AntiVirus Professional Edition**.
4. Do one of the following:
   - In Windows 2000/Me, click **Change/Remove**.
   - In Windows 98, click **Add/Remove**.
   - In Windows XP, click **Change**.
5. Click **Yes** to confirm that you want to uninstall the product.
6. If you have files in Quarantine, you are asked if you want to delete them. Your options are:

See "If you have files in Quarantine" on page 78.

Yes	Deletes the quarantined files from your computer.
No	Leaves the quarantined files on your computer, but makes them inaccessible.

7 Click **Finish**.


Installer Information
You must restart your system for the configuration changes made to Norton AntiVirus 2003 Professional Edition to take effect. Click Yes to restart now or No if you plan to manually restart later.
Yes
No

8 Click **Yes** to restart your computer.

To uninstall Norton AntiVirus Professional Edition from the Programs menu

1 Do one of the following:
- On the Windows taskbar, click **Start** > **Programs** > **Norton AntiVirus**.
- On the Windows XP taskbar, click **Start** > **All Programs** > **Norton AntiVirus**.

2 Click **Uninstall Norton AntiVirus 2003 Professional Edition**.

3 On the Application Maintenance window, click **Remove**.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate.

To uninstall LiveReg and LiveUpdate

1 Do one of the following:
- On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
- On the Windows XP taskbar, click **Start** > **Control Panel**.

2 In the Control Panel, double-click **Add/Remove Programs**.

3 In the list of currently installed programs, click **LiveReg**.

4 Do one of the following:
- In Windows 2000/Me, click **Change/Remove**.
- In Windows 98, click **Add/Remove**.
- In Windows XP, click **Remove**.

5 Click **Yes** to confirm that you want to uninstall the product.

6 Repeat steps 1 through 5, selecting LiveUpdate in step 3, to uninstall LiveUpdate.

Norton AntiVirus Professional Edition basics

3

Norton AntiVirus Professional Edition basics include general information about how to access Norton AntiVirus Professional Edition tools, keep your computer protected, customize Norton AntiVirus Professional Edition, monitor Norton AntiVirus Professional Edition activities and access more information about Norton AntiVirus.

Access Norton AntiVirus Professional Edition tools

Norton AntiVirus Professional Edition tools include status reporting, scanning options, scheduling options, activity reporting, file recovery and permanent file removal, and configuration options for your computer. Access these tools from the Norton AntiVirus Professional Edition main window, the Windows Explorer toolbar, and the Norton AntiVirus Windows tray *icon*.

Use the Norton AntiVirus Professional Edition main window

Most tools are available from the Norton AntiVirus Professional Edition main window.

To start Norton AntiVirus Professional Edition on your computer

- Do one of the following:
  - On the Windows taskbar, click **Start** > **Programs** > **Norton AntiVirus** > **Norton AntiVirus 2003 Professional Edition**.
  - On the Windows XP taskbar, click **Start** > **All Programs** > **Norton AntiVirus** > **Norton AntiVirus 2003 Professional Edition**.

Use the Windows Explorer toolbar

Norton AntiVirus Professional Edition adds a button and menu to Windows Explorer. The button drops down an abbreviated Norton AntiVirus menu. Click the arrow to the right of the button and the following options appear.

View Status	Launches Norton AntiVirus, displaying the Status pane with system status.
View Quarantine	Displays the Quarantine area and the files currently stored there. For more information, see "If you have files in Quarantine" on page 78.
View Activity Log	Displays the Activity Log, showing you various Norton AntiVirus activities, such as scans performed and problems found. For more information, see "Keeping current with LiveUpdate" on page 65.
View Virus Encyclopedia	Connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.
Scan for Viruses	Opens Norton AntiVirus in the Scan for Viruses pane, on which you can specify a scan to run.

When you first open Windows Explorer after installing Norton AntiVirus Professional Edition, you may not see the Norton AntiVirus button and menu.

To display the Norton AntiVirus button and menu

- On the View menu, click **Toolbars** > **Norton AntiVirus**.

You may not be able to access the Norton AntiVirus Professional Edition Windows Explorer menu, depending on your computer's configuration.

Use the Norton AntiVirus Windows tray icon

See "Customize Norton AntiVirus Professional Edition" on page 44.

You can use the Norton AntiVirus Professional Edition *icon* in the Windows tray to open Norton AntiVirus, and enable or disable Auto-Protect.

To use the Norton AntiVirus Windows tray icon

1. In the Windows tray, right-click the Norton AntiVirus icon.
2. On the tray icon menu, select the option that you want.

Check the version number

You can check the version number of Norton AntiVirus Professional Edition on your computer.

To check the version number

1. Start Norton AntiVirus Professional Edition.
2. Click **Help** > **About Norton AntiVirus Professional**.
3. Click **Norton AntiVirus**.

Temporarily disable Auto-Protect

See "Customize Norton AntiVirus Professional Edition" on page 44.

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. When a virus or *virus-like activity* is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect on your computer.

If you have set a *password* for Options, Norton AntiVirus Professional Edition asks you for the password before you view or adjust the settings.

To temporarily disable Auto-Protect on your computer

See "Access Norton AntiVirus Professional Edition tools" on page 37.

1. Start Norton AntiVirus Professional Edition.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options dialog box, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, uncheck **Enable Auto-Protect**.

Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

To enable Auto-Protect

1. Start Norton AntiVirus Professional Edition.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options dialog box, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton AntiVirus *icon* appears in the Windows tray, you can use it to enable and disable Auto-Protect.

To enable or disable Auto-Protect on your computer using the tray icon

1. In the Windows tray, right-click the Norton AntiVirus icon.
2. Do one of the following:
   - If Auto-Protect is enabled, click **Disable Auto-Protect**.
   - If Auto-Protect is disabled, click **Enable Auto-Protect**.

Maintain Norton AntiVirus Professional Edition protection

See "If you need to use Rescue Disks (Windows 98/98SE/Me)" on page 80.

Depending upon which *operating system* you are using, you may want to keep a set of Rescue Disks available and keep them up-to-date. You should also occasionally verify that Norton AntiVirus Professional Edition is set to provide you with optimal protection, and make sure that your virus protection is current.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue items and a virus scanner across multiple floppy disks or on a network drive. Rescue Disks can be made for Windows 98/Me operating systems; they are not needed for Windows 2000/XP.

A Rescue Disk set consists of one bootable floppy disk, one Norton AntiVirus Program floppy disk, and three Virus Definition floppy disks. If you have Norton Utilities installed, you will also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start

your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

Rescue Disks contain information specific to the computer on which they were made. If you are using Rescue Disks for recovery, you must use the disks made for your computer. If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer.

See "If you need to use Rescue Disks (Windows 98/98SE/Me)" on page 80.

Rescue Disks can and should be updated whenever you update your virus protection, install new software, or make changes to your hardware.

Create a Rescue Disk set

Rescue Disks can be created at any time. If you have chosen to create Rescue Disks as a post-install task in the Information Wizard, the Rescue Disk Wizard appears automatically. Otherwise, you can start the Rescue Disk Wizard from the Norton AntiVirus Professional Edition main window.

See "Temporarily disable Auto-Protect" on page 39.

If you start the Rescue Disk Wizard from the Norton AntiVirus Professional Edition main window, temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again.

You will need several formatted 1.44-MB disks.

To create Rescue Disks

1. Start Norton AntiVirus Professional Edition.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Rescue**.
   If you chose to make Rescue Disks as a post-install task, the Rescue Disk Wizard opens automatically.
3. Select drive A to create the Rescue Disk set.
4. Click **Create**.
5. Label the disks as specified in the Basic Rescue Disk List window, then click **OK**.
6. Insert the disks as requested.

Test your Rescue Disks

At the end of the Create Rescue Disks process, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.

To test your Rescue Disks

1. Close all open Windows programs.
2. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.

   If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly. If the Rescue Disk screen does not appear, you have several options for correcting the problem.

See "My Rescue Disk does not work" on page 95.

3. Press **Escape** to exit to DOS.
4. Remove the disk from drive A, then slide open the plastic tab on the back of the disk to write-protect it.
5. Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. Rescue Disk lets you update your basic Rescue Disks without having to recreate them.

If you are updating a floppy disk set, make sure your disks are not write-protected before you begin.

To update your Rescue Disks

1. Start Norton AntiVirus Professional Edition.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Rescue**.
3. Under Select Destination Drive, select drive A.
4. Click **Update**.
5. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.
6. Click **OK**.
7. Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted.

See "Test your Rescue Disks" on page 41.

Check system status

If Norton AntiVirus Professional Edition is behaving in an unexpected way, or if you're not sure that your computer is being scanned for viruses, check the status of your configuration.

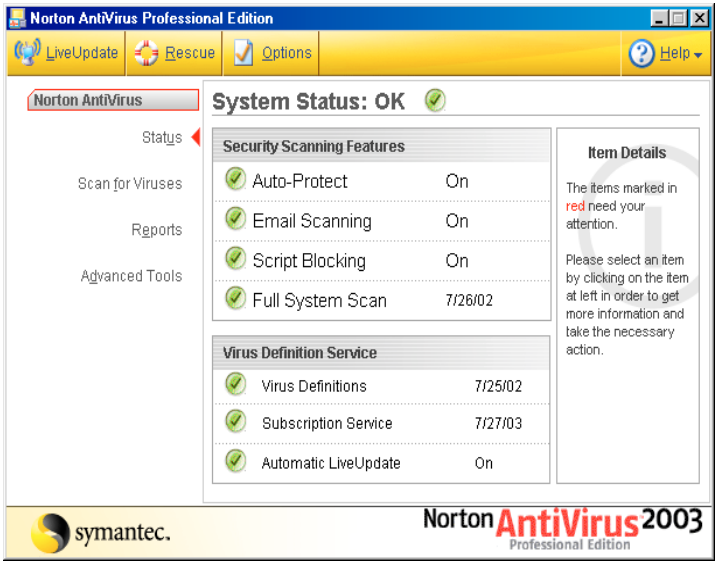
In the Status pane of the Norton AntiVirus Professional Edition main window, a check mark indicates that the system status is OK and a triangle indicates that your system needs attention. If you see a triangle, review the features and services to see which area needs attention.

If you need to adjust any settings use Options. See "Customize Norton AntiVirus Professional Edition" on page 44.

To check system status

See "Access Norton AntiVirus Professional Edition tools" on page 37.

1 Start Norton AntiVirus Professional Edition.



2 In the Status window, review the status to the left of each feature.

3 For more information about a particular feature, click the feature. The right pane displays a description and a link to more information about the feature.

Check Office Plug-in status

Office Plug-in protects Microsoft Office documents. It scans those documents whenever you open them in a Microsoft Office program. Office Plug-in is enabled in Options.

If you have set a password for Options, Norton AntiVirus Professional Edition asks you for the password before you can view or adjust the settings.

To check Office Plug-in status

See "Access Norton AntiVirus Professional Edition tools" on page 37.

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the left pane of the Options window, under Other, click **Miscellaneous**.
4. Verify that Office Plug-in is enabled.

Customize Norton AntiVirus Professional Edition

If you are using Windows 2000/XP and you do not have Local Administrator access, you cannot change Norton AntiVirus Professional Edition options. If you are an Administrator and share your computer with others, keep in mind that the changes you make apply to everyone using the computer.

The default settings for Norton AntiVirus Professional Edition provide complete virus protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

Norton AntiVirus Professional Edition provides password protection for your option settings. You can enable, change and reset a password so unauthorized users cannot tamper with your settings.

All the settings for Options are organized into three main categories. The options contained under each category are as follows.

Category	Options
System	Auto-Protect ▪ Bloodhound ▪ Advanced ▪ Exclusions Script Blocking Manual Scan ▪ Bloodhound ▪ Exclusions
Internet	Email ▪ Advanced Instant Messenger LiveUpdate
Other	Inoculation (Windows 98/98SE/Me) Miscellaneous Advanced Tools

See "Change Norton AntiVirus Professional Edition options" on page 48.

This section does not describe how to change the individual options, but gives a general description of what they do and how you can find them. For specific information about an option, check the online Help.

About System options

The System options control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight tradeoff in computer performance. If you notice a difference in your computer's performance after you install Norton AntiVirus Professional Edition, you may want to set protection to a lower level or disable those options that you do not need.

Option	Description
Auto-Protect	Determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what to do when a virus is found. Bloodhound is the scanning technology that protects against unknown viruses. Use these options to set its level of sensitivity in Auto-Protect. Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks. Exclusions specify the files that should not be scanned by file name extension or by specific file name. Be careful not to exclude the types of files that are more likely to be infected by viruses such as files with macros or executable files.
Script Blocking	Enable Script Blocking and set what Norton AntiVirus Professional Edition should do if it finds a malicious script. If you are developing or debugging scripts, disable Script Blocking. Otherwise this feature might block the script you are developing.
Manual Scan	Determine what gets scanned and what happens if a virus is found during a scan that you request. Manual Scan options also include Bloodhound and Exclusions subcategories.

About Internet options

Internet options define what happens when your computer is connected to the Internet. You use Internet options to define how Norton AntiVirus Professional Edition should scan email and instant messenger attachments, enable Worm Blocking, and determine how LiveUpdates should be applied.

Option	Description
Email	Enable email scanning and Worm Blocking, and define how Norton AntiVirus Professional Edition should behave while scanning email messages. Scanning incoming email protects your computer against viruses sent by others. Scanning outgoing email prevents you from inadvertently transmitting viruses or worms to others. You can choose to scan incoming or outgoing email, or both, and to display an icon or progress indicator while scanning. You can set options to automatically repair, quarantine, or delete infected email with or without interaction with you. Advanced options determine what to do when scanning email.
Instant Messenger	Determine what instant messengers to support, how to configure a new IM, and what happens if a virus is found during an instant messenger session.
LiveUpdate	Enable Automatic LiveUpdate and define how updates should be applied. Automatic LiveUpdate checks for updated virus definitions and program updates automatically when you are connected to the Internet.

About Other options

Other options include Inoculation settings for Windows 98/98SE/Me and Miscellaneous settings. You can enable Inoculation, cause an alert if a system file changes, and set a variety of miscellaneous options.

Option	Description
Inoculation	Enable inoculation and, if a system file changes, choose to update the inoculation snapshot or repair the file by restoring it to its original values. Inoculation options are available only on Windows 98/98SE/Me.
Miscellaneous	Back up file in Quarantine before attempting a repair. (This option is automatically set to On.) Enable Office Plug-in. If you upgrade to Microsoft Office 2000 or later after Norton AntiVirus Professional Edition is installed, you must enable this option to automatically scan Microsoft Office files. Alert me if my virus protection is out of date. Scan files at system startup (Windows 98/98SE only). Enable password protection for options.
Advanced Tools	Customize the behavior and name of desktop icon for the Norton recycle bin. Enable or disable and customize Norton Protection for deleted files.

Change Norton AntiVirus Professional Edition options

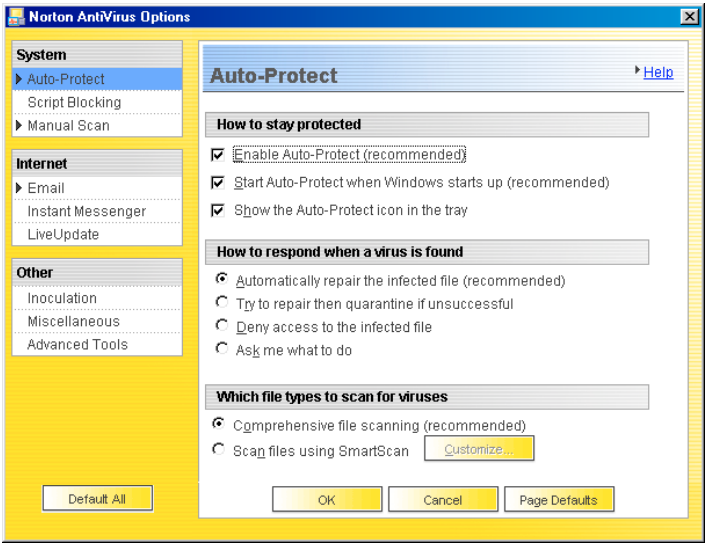
You change the settings for Norton AntiVirus Professional Edition options in the Options window.

To change settings

See "Access Norton AntiVirus Professional Edition tools" on page 37.

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus main window, click **Options**.

If you set a password for Options, Norton AntiVirus Professional Edition asks you for the password before you can continue.



3 In the Options window, in the left pane, click an option in the list. Options with an arrow to the left have sub-options. As you click an option, the corresponding settings for the selected option appear in the right pane.

4 Select any settings you want to change.

5 Click **OK**.
These settings now take precedence over the preset options. The changes take effect immediately.

See "Customize Norton AntiVirus Professional Edition" on page 44.

If you need to restore default settings in Options

You can change any or all of the options listed. If you have made a number of changes that have unwanted results, you can restore all options to the default settings.

If you set a password for Options, Norton AntiVirus Professional Edition asks you for the password before you can view or adjust the settings.

To restore default settings on an Options page

- On the page for which you want to restore default settings, click **Page Defaults**.

To restore default settings for all options

- On any page in the Options window, click **Default All**.

Password protect Norton AntiVirus options

You can choose to protect or remove protection from your option settings with a password. If you specify a password, you are asked to enter a password every time you view the Options window, or temporarily enable or disable Auto-Protect.

If you forget your password, you can reset it from the Help button in the Norton AntiVirus main window. Check online Help for more information about resetting your password.

To specify or remove a password

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under Other, click **Miscellaneous**.
4. Check or uncheck **Enable password protection for options**.
5. In the password dialog box, enter a password.
6. Click **OK**.

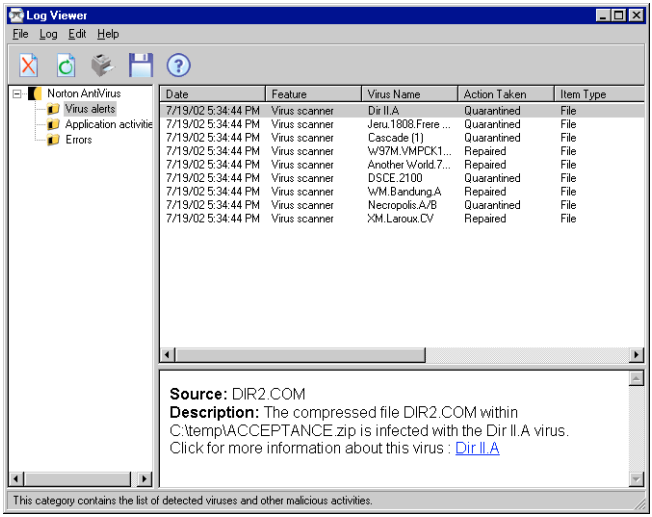
Monitoring Norton AntiVirus Professional Edition activities

Occasionally, you may need to look at previous Norton AntiVirus Professional Edition activities, such as when the last system scan was done or how many viruses were detected last week. Norton AntiVirus Professional Edition displays a record of its virus detection, application, and error activities in the *Log* Viewer.

Check the Activity Log to see what tasks Norton AntiVirus Professional Edition has performed and the results of those tasks to make sure your Options settings are set correctly for your particular needs.

To check activities

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Reports**.
3. In the Reports pane, on the Activity Log line, click **View Report**.


Log Viewer
File Log Edit Help
Norton AntiVirus
Virus alerts
Application activitie
Errors
Date Feature Virus Name Action Taken Item Type
7/19/02 5:34:44 PM Virus scanner Dir II.A Quarantined File
7/19/02 5:34:44 PM Virus scanner Jeru.1808.Frere ... Quarantined File
7/19/02 5:34:44 PM Virus scanner Cascade (1) Quarantined File
7/19/02 5:34:44 PM Virus scanner W97M.VMPCK1... Repaired File
7/19/02 5:34:44 PM Virus scanner Another World.7... Repaired File
7/19/02 5:34:44 PM Virus scanner DSCE.2100 Quarantined File
7/19/02 5:34:44 PM Virus scanner WM.Bandung.A Repaired File
7/19/02 5:34:44 PM Virus scanner Necropolis.A/B Quarantined File
7/19/02 5:34:44 PM Virus scanner XM.Laroux.CV Repaired File
Source: DIR2.COM
Description: The compressed file DIR2.COM within C:\temp\ACCEPTANCE.zip is infected with the Dir II.A virus.
Click for more information about this virus : Dir II.A
This category contains the list of detected viruses and other malicious activities.

4. In the left pane, click the log you want to review.
   As you click each log, the right pane changes and displays information specific to the particular log. The most recent activities appear at the top of the log.

For more information

Norton AntiVirus Professional Edition provides glossary terms, online Help, this User's Guide in PDF format, tutorials on the Web, and links to the Knowledge Base on the Symantec Web site.

Look up glossary terms

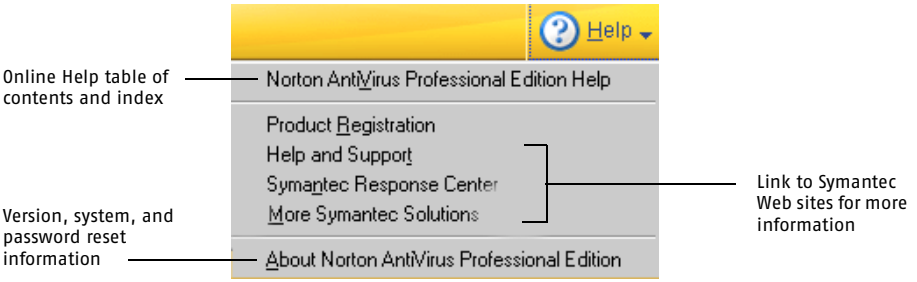
Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is always available throughout Norton AntiVirus Professional Edition. Help buttons or links to more information provide information specific to the task you are completing. The Help menu provides a comprehensive guide to all product features and tasks you can complete.

To access the Help menu

1. Start Norton AntiVirus Professional Edition.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Help**.


Help
Online Help table of contents and index
Norton AntiVirus Professional Edition Help
Product Registration
Help and Support
Symantec Response Center
More Symantec Solutions
Link to Symantec Web sites for more information
Version, system, and password reset information
About Norton AntiVirus Professional Edition

3. On the main Help menu, click **Norton AntiVirus Professional Edition Help**.
4. In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search field where you can enter a word or phrase

Help for Norton AntiVirus Professional Edition dialog boxes

When you request Help while working in a Norton AntiVirus Professional Edition dialog box, the Help displayed is specific to that dialog box.

To get Help for a Norton AntiVirus Professional Edition dialog box

- In the dialog box, click **Help**.

Help for a specific task

Online Help also explains procedures that you are likely to perform using Norton AntiVirus Professional Edition. You can access these topics from the main Help window.

To get Help for a task

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Help**.
3. On the main Help menu, click **Norton AntiVirus Professional Edition Help**.
4. In the Help window, in left pane, select a tab. Your options are:

Contents	Search for Help by topic.
Index	Lists Help topics in alphabetical order by key word.
Search	Enter and search for Help by key word.

The Contents, Index, and Search tabs are also available in many other Help windows and can always be used to search for Help.

Use the User's Guide PDF

This User's Guide is provided on the Norton AntiVirus Professional Edition CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.

To install Adobe Acrobat Reader

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click the **Acrobat** folder.
5. Double-click **AR500ENU**.
6. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

To read the User's Guide PDF from the CD

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click the **NAP2003** folder.
5. Double-click **NAP2003.pdf**.

You can also copy the User's Guide to your hard disk and read it from there. It needs approximately 1 MB of disk space.

To read the User's Guide from your hard disk

1. Open the location into which you copied the PDF.
2. Double-click **NAP2003.pdf**.

About Norton AntiVirus Professional Edition on the Web

The Symantec Web site provides extensive information about Norton AntiVirus Professional Edition, virus protection, antivirus technology, and other Symantec products. There are several ways to access the Symantec Web site.

To access the Symantec Web site from the Norton AntiVirus Professional Edition main window

1. Click **Help**.
2. Select the solution that you want. Your options are:

Help and Support	Takes you to the technical support page of the Symantec Web site, from which you can search for solutions to specific problems, update your virus protection, and read the latest information about antivirus technology.
Symantec Response Center	Takes you to the Symantec security response page of the Symantec Web site, from which you can get the latest virus threats and security updates.
More Symantec Solutions	Takes you to the Symantec store page of the Symantec Web site, from which you can get the latest product information and shop for Symantec products.

The Reports pane of Norton AntiVirus Professional Edition contains a link to the Symantec online virus encyclopedia.

To access the Symantec Web site from the Reports page

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Reports**.
3. In the Reports pane, next to the Online Virus Encyclopedia heading, click **View Report**.

There is a link to the Symantec Web site on the Windows Explorer toolbar.

To access the Symantec Web site from Windows Explorer

1. Open Windows Explorer.
2. On the toolbar, on the Norton AntiVirus Professional Edition menu, click **View Virus Encyclopedia**.
   This option connects you to the Symantec security response Web page, from which you can search for information on all types of viruses.

You can always access the Symantec Web site through your Internet *browser*.

To access the Symantec Web site in your browser

- Point your browser to www.symantec.com

Explore online tutorials

Symantec provides online tutorials that you can use to review many common tasks that Norton AntiVirus Professional Edition performs.

To explore the online tutorials

1. Point your browser to www.symantec.com/techsupp/tutorials.html
2. On the tutorials Web page, select the product and version for which you want a tutorial.
3. Click **continue**.
4. In the list of available tutorials for your product, select the one that you want to review.

Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special virus definition releases.

To subscribe to the Symantec Security Response newsletter

1. Point your browser to securityresponse.symantec.com
2. On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
3. On the security response newsletter Web page, choose the language in which you want to receive the newsletter.
4. Under subscribe, type the information requested, then click **Subscribe**.

Protecting disks, files, and data from viruses

4

Keeping your computer protected requires regular monitoring by Auto-Protect, Script Blocking, and Worm Blocking; scanning of your *email* attachments and files transferred by instant messenger; and frequent system scans. All of these tasks can be set to occur automatically.

For added protection in Norton AntiVirus on Windows 98/98SE/Me, enable inoculation to *alert* you if a system file changes.

Ensure that protection settings are enabled

Norton AntiVirus Professional Edition is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, for maximum protection, you should ensure that your protection features are enabled.

Feature	Where to set	Maximum protection setting
Auto-Protect	**Norton AntiVirus main window** > **Enable**	Auto-Protect is set to **On**.
Email scanning	**Options** > **Email** See "About Internet options" on page 47.	**Scan incoming Email** and **Scan outgoing Email** are checked. If your email program uses one of the supported communications protocols, both options are selected by default.

Feature	Where to set	Maximum protection setting
Timeout protection	**Options** > **Email** See "About Internet options" on page 47.	**Protect against timeouts when scanning Email** is checked. To prevent connection timeouts while receiving large attachments, enable timeout protection.
Instant messenger scanning	**Options** > **Instant Messenger** See "About Internet options" on page 47.	Instant messengers that you want to protect are checked.
Worm Blocking	**Options** > **Email** See "About Internet options" on page 47.	**Enable Worm Blocking** and **Alert me when scanning email attachments** are checked.
Script Blocking	**Options** > **Script Blocking** See "About System options" on page 45.	**Enable Script Blocking** is checked.
Inoculation	**Options** > **Inoculation** See "About Other options" on page 48.	**Inoculate Boot Records** is checked.

This table summarizes the maximum protection settings and where you can find them. For specific information about an option, check the online Help.

Manually scan disks, folders, and files

If Auto-Protect is enabled and the Norton AntiVirus options are set at their default levels, you normally would not need to scan manually. However, if you temporarily disabled Auto-Protect (for example, to load or use another program that conflicts with Norton AntiVirus), and you forgot to enable it again, it is possible that a virus could be on your hard disk undetected. You can scan your entire computer, or individual floppy disks, drives, folders, or files.

Although the default settings for manual scanning are usually adequate, you can raise the level of Bloodhound heuristics or adjust the options for

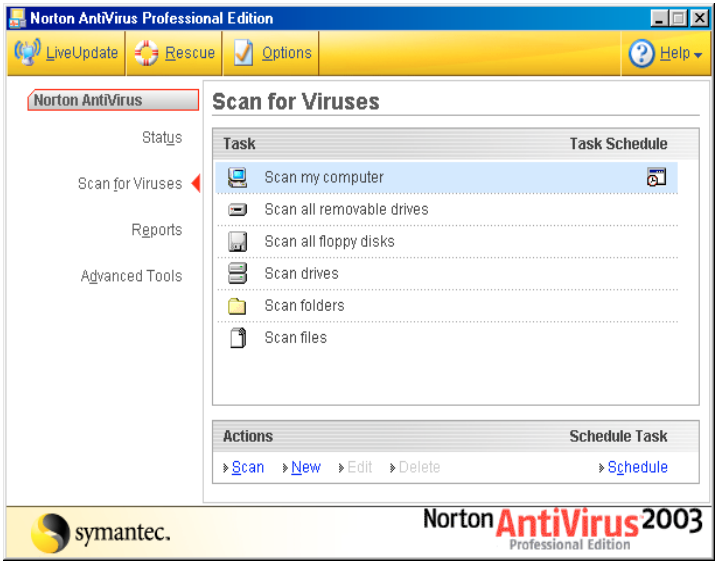
manual scanning in the Options window. Check online Help for more information about manual scanning options.

Perform a full system scan

A full system scan scans all *boot records* and files on your computer.

To perform a full system scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.



3. In the Scan for Viruses pane, click **Scan my computer**.
4. Under Actions, click **Scan**.
   When the scan is complete, a scan summary appears.
5. When you are done reviewing the summary, click **Finished**.

Scan individual elements

Occasionally, you may want to scan a particular file, removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer. You may have been working with floppy disks or have received a compressed file in an email message and suspect a virus. You can scan just a particular disk or individual element that you want to check.

To scan individual elements

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to run.
4. Under Actions, click **Scan**.
   If you choose to scan all removable drives or a floppy disk, the scan starts automatically. If you choose to scan drives, folders, or files, a dialog box appears in which you choose which drives, folders, or files to scan.
5. In the dialog box, click **Scan** after making your selection.
   When the scan is complete, a scan summary appears.
6. When you are done reviewing the summary, click **Finished**.

If problems are found during a scan

See "If a virus is found during a scan" on page 73.

At the end of a scan, a summary report appears to tell you what Norton AntiVirus Professional Edition found during the scan. If a virus was found and you have requested that Norton AntiVirus Professional Edition repair the file automatically, it is listed as repaired. If the file cannot be repaired, it can be quarantined or deleted.

Create and use custom scans

See "Schedule a custom scan" on page 62.

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can also schedule the custom scan to run automatically.

You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

To create a custom scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, under Actions, click **New**.

4. In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.
5. Do one or both of the following:
   - To select individual files to be scanned, click **Add files**.
   - To select folders and drives to be scanned, click **Add folders**.

   You can use both options to select the combination of items that you want.
6. In the resulting dialog box, select the items that you want to scan.
   If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.
7. Add the selected items to the list of items to scan by doing one of the following:
   - In the Scan Files dialog box, click **Open**.
   - In the Scan Folders dialog box, click **Add**.
8. To remove an item from the list, select it, then click **Remove**.
9. When you are done creating the list of items to be scanned, click **Next**.
10. Type a name for the scan by which you can identify it in the list of scans.
11. Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the custom scan.
4. Under Actions, click **Scan**.
   When the scan is complete, a scan summary appears.
5. When you are done reviewing the summary, click **Finished**.

Delete a custom scan

You can delete custom scans if they are no longer needed.

To delete a custom scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to delete.

If you click the button next to the scan name, the scan runs.

4. Under Actions, click **Delete**.
5. Click **Yes** to verify that you want to delete the scan.

Schedule scans

When you install Norton AntiVirus Professional Edition and complete the Information Wizard, you can choose to schedule a weekly full system scan as part of post-install tasks. If you make that choice, the scan is scheduled automatically.

You can schedule customized virus scans that run unattended on specific dates and times or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working.

You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a custom scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to schedule.

If you click the button next to the scan name, the scan runs.

4. Under Schedule Task, click **Schedule**.
5. In the Schedule dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.
   If it is not checked, the fields are already enabled.
6. Set the frequency and time at which you want the scan to run.
   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
7. When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to schedule.

If you click the button next to the scan name, the scan runs.

4. Under Schedule Task, click **Schedule**.
5. In the Schedule dialog box, check **Show multiple schedules**.
6. To set an additional schedule, click **New**.
7. Set the frequency and time at which you want the scan to run.
   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
8. When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to schedule.

If you click the button next to the scan name, the scan runs.

4. Under Schedule Task, click **Schedule**.
5. Change the schedule as desired.
6. Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan you want to schedule.

If you click the button next to the scan name, the scan runs.

4. Under Schedule Task, click **Schedule**.
5. In the Schedule dialog box, check **Show multiple schedules**.
6. Select the schedule that you want to delete (if more than one).
7. Click **Delete**.
8. Click **OK**.

Keeping current with LiveUpdate

5

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.

If you are using Norton AntiVirus Professional Edition on Windows 2000/XP, you must have Administrator access rights to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files available from Symantec, by subscription, that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton SystemWorks	Users of Norton AntiVirus and Norton SystemWorks receive virus definition service updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security	In addition to the virus definition service, users of Norton Internet Security also receive protection updates to the Web filtering service, the intrusion detection service, and Spam Alert. The Web filtering service updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content. The intrusion detection service updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer. Spam Alert updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection service updates for the latest predefined firewall rules and updated lists of applications that access the Internet.

About your subscription

See "Subscription policy" on page 102.

Your Symantec product includes a complimentary, limited-time subscription to protection updates for the subscription services that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates and will not be protected against newly discovered threats.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Request an update alert

To ensure your protection updates are current, you can request to receive an email alert whenever there is a high-level virus outbreak or other Internet security threat. The email alert describes the threat, provides detection and removal instructions, and includes advice on keeping your computer safe. You should always run LiveUpdate after you receive one of these alerts.

To request an update alert

1. From your Web browser, navigate to securityresponse.symantec.com/avcenter
2. On the Security Response Web page, scroll to the bottom of the page, then click **Symantec security response Free subscription**.
3. On the security alert subscription Web page, fill in the subscription form.
4. Click **Send me FREE Security Alerts**.

If you run LiveUpdate on an internal network

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

Your subscription must be current to obtain new protection updates from the Symantec Web site.

To obtain updates from the Symantec Web site

1. Point your Web browser to securityresponse.symantec.com
2. Follow the links to obtain the type of update that you need.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.

If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.
   You might receive a warning that says that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. In the LiveUpdate window, click **Next** to locate updates.
4. If updates are available, click **Next** to download and install them.
5. When the installation is complete, click **Finish**.

Some program updates may require that you restart your computer after you install them.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate downloads a list of updates available for your Symantec products that are supported by LiveUpdate technology. You can then choose which product updates you want to install. In Express mode,

LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.
3. On the LiveUpdate welcome screen, click **Configure**.
4. On the General tab of the LiveUpdate Configuration dialog box, select **Interactive Mode** or **Express Mode**.
5. If you selected Express Mode, select how you want to start checking for updates:
   - To have the option of cancelling the update, select **I want to press the start button to run LiveUpdate**.
   - To have any updates installed automatically whenever you start LiveUpdate, select **I want LiveUpdate to start automatically**.
6. Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Symantec LiveUpdate**.
3. On the General tab of the LiveUpdate Configuration dialog box, select **Interactive Mode**.
4. Click **OK**.

Run LiveUpdate automatically

You can have LiveUpdate check for protection updates automatically, on a set schedule, by enabling Automatic LiveUpdate. You must continue to run LiveUpdate manually to receive product updates.

Automatic LiveUpdate checks for an Internet connection every five minutes until a connection is found, and then every four hours. If you have an ISDN router that is set to automatically connect to your Internet service provider (ISP), many connections will be made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate in the Norton AntiVirus Professional Edition options.

To enable Automatic LiveUpdate

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.

   If you set a password for Options, Norton AntiVirus Professional Edition asks you for the password before you can continue.
3. In the Options window, under Internet, click **LiveUpdate**.
4. In the LiveUpdate pane, check **Enable Automatic LiveUpdate**.
5. Set how you want updates to be applied. Your options are:

Apply updates without interrupting me	LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate displays an alert when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
Notify me when updates are available	LiveUpdate checks for protection updates and asks if you want to install them.

6. Click **OK**.

To delete the schedule for Automatic LiveUpdate, disable Automatic LiveUpdate.

To disable Automatic LiveUpdate

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.

If you set a password for Options, Norton AntiVirus Professional Edition asks you for the password before you can continue.

3. In the Options window, under Internet, click **LiveUpdate**.
4. In the LiveUpdate pane, uncheck **Enable Automatic LiveUpdate**.
5. Click **OK**.

What to do if a virus is found

6

If Norton AntiVirus Professional Edition finds a virus on your computer, there are three possible resolutions to the problem:

- Fix the file
  Removes the *virus* from the file or if the *threat* is a worm or Trojan horse, deletes the file.
- Quarantine the file
  Makes the file inaccessible by any programs other than Norton AntiVirus. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
- Delete the file
  Removes the virus from your computer by deleting the file that contains the virus, worm or Trojan horse. It should be used only if the file cannot be repaired or quarantined.

See "If you have files in Quarantine" on page 78.

Malicious *threats* can be found during a manual or scheduled scan or by Auto-Protect when you perform an action with an *infected file*. Threats can also appear during an instant messenger session or when sending an email. The way that you handle a threat differs depending on whether a scan or Auto-Protect found the threat.

If a virus is found during a scan

If Norton AntiVirus Professional Edition finds a virus, Trojan horse, or worm during a scan or from an instant messenger session, you either receive a summary of the automatic repair or deletion results, or you have to use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus Professional Edition repairs files automatically, and all infected files could be repaired, the Scan Summary lists the number of files infected and repaired. This information is presented for status purposes only; you don't need to take further action to protect your computer. If you want to know more, you can check the repair details to see which files were infected and with what threats.

To review the repair details

1. In the scanner window, in the Summary pane, click **More Details**.
2. When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be fixed, or if you have set your manual scan options so that Norton AntiVirus Professional Edition asks you what to do when a virus is found, the Repair Wizard opens. If Norton AntiVirus Professional Edition did not attempt a repair, the Repair Wizard opens in the Repair pane. Otherwise, it opens in the Quarantine window.

To use the Repair Wizard

1. If the Repair Wizard opens in the Repair pane, uncheck any files that you don't want Norton AntiVirus Professional Edition to fix.
   All files are checked by default. This is the recommended action.
2. Click **Fix**.
   If any files cannot be fixed or deleted, the Quarantine window opens.
   All files are checked to be added to the Quarantine by default. This is the recommended action.
3. In the Quarantine window, uncheck any files that you do not want to quarantine.
4. Click **Quarantine**.
   If any files could not be quarantined, the Delete pane opens.
   If you do not delete the infected files, the virus remains on your computer and can cause damage or be transmitted to others.
5. Uncheck any files that you do not want to delete.

6 Click **Delete**.
Once all of the files have been repaired, quarantined, or deleted, the Summary pane of the scanner window opens.

7 When you are done reviewing the summary, click **Finished**.

After repairing a boot virus on your hard drive, restart your computer.

If a virus is found by Auto-Protect

Auto-Protect scans files for viruses and other malicious *threats* when you perform an action with them, such as moving them, copying them, or opening them. If it detects a virus or virus-like activity, in most cases you receive an *alert* telling you that a virus was found and repaired. How you proceed depends on the *operating system* that you are using.

If you are using Windows 98/98SE/Me

If a virus or threat is found and repaired by Auto-Protect in Windows 98/98SE/Me, you receive an alert telling you which file was repaired or deleted.

To close the alert

❖ Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose an action. The recommended action is always preselected.

Action	Result
Repair the infected file	Automatically eliminates the virus, Trojan horse, or worm and repairs or deletes the infected file. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the infected file, but does not remove the threat. Select Quarantine if you suspect that the infection is caused by an unknown threat and you want to submit the threat to Symantec for analysis.
Delete the infected file	Erases both the threat and the infected file. Select Delete if Repair is not successful. Replace the deleted file with the original program file or backup copy. If the virus, Trojan horse, or worm is detected again, your original copy is infected.

Action	Result
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time that you perform the same activity.
Ignore the problem and do not scan this file in the future	Adds the file that is suspected of containing a threat to the Exclusions list. When you add a file to the Exclusions list, the file is excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this option only if you are sure that a virus, Trojan horse or worm is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If a file cannot be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows 2000/XP

If a *threat* is found and either repaired or automatically deleted by Auto-Protect in Windows 2000/XP, you receive an alert telling you which file was repaired or deleted and which virus, Trojan horse, or worm was infecting the file. If you have an active Internet connection, clicking the virus name opens the Symantec Web page that describes the virus.

To close the alert

❖ Click **OK**.

If the file cannot be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file, and another telling you that access to the file was denied.

See "If you have files in Quarantine" on page 78.

You can set your Auto-Protect options to try to quarantine any infected files that it cannot repair. If you do this, you are informed if any files are quarantined.

To resolve problems with unrepaired files

See "Perform a full system scan" on page 59.

1 Run a full system scan on your computer to ensure that no other files are infected.

See "If a virus is found during a scan" on page 73.

2 Follow the recommended actions in the Repair Wizard to protect your computer from the infected files.

If a virus is found by Script Blocking

See "Ensure that protection settings are enabled" on page 57.

Script Blocking scans Visual Basic and JavaScript scripts for viruses. If it detects a virus or virus-like activity, in most cases you receive an alert telling you that a potential *threat* was found.

You must choose one of the options to remove the threat. The recommended action is to stop the script from running. You can click Help on the alert for additional information about how to respond.

If a threat is found by Worm Blocking

See "Ensure that protection settings are enabled" on page 57.

If a program tries to email itself or email a copy of itself, it could be a worm trying to spread via email. A worm can send itself or a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for *worms*. If it detects a worm, you receive an alert telling you that a malicious worm was found.

The alert presents you with options and asks you what to do. If you were not sending an email message at that time, then it is probably a worm and you should quarantine the file. You can click Help on the alert for additional information about how to respond.

After you have responded to the *threat* and deleted the file, you could still have an infected system. Run LiveUpdate, scan your system, and, if necessary, go to the Symantec security response Web page (securityresponse.symantec.com) for the most up-to-date virus definitions clean-up tools.

If Inoculation alerts you about a change in system files

Inoculation protection is available on Windows 98/98SE/Me systems only.

See "Ensure that protection settings are enabled" on page 57.

System files can change for a variety of reasons. You may have updated your *operating system* or repartitioned your hard disk, or you could have a virus. Norton AntiVirus alerts you when a change occurs in your system files.

If you get an *alert* about a change in your system files, you have two options. You can update your inoculation snapshot or repair the file. Before you repair the file, be sure your virus definitions are up-to-date and run a scan.

To respond to inoculation changes

- In the Alert window, select the action that you want to take. Your options are:

Update the saved copy of my Master Boot Record	Use if the alert appears after a legitimate change in system files.
Restore my Master Boot Record	Use if you are certain the system did not change for legitimate reasons.

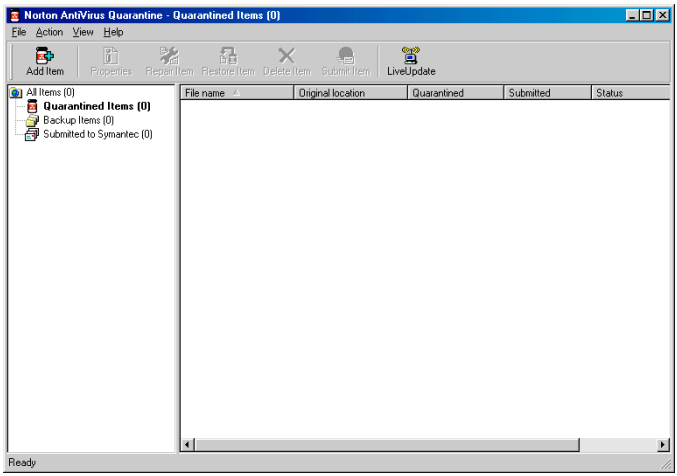
If you have files in Quarantine

Once a file has been placed in Quarantine, you have several options. All actions that you take on files in Quarantine must be performed in the Quarantine window.

To open the Quarantine window

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Reports**.

3 In the Reports pane, on the Quarantined items line, click **View Report**.



The toolbar at the top of the Quarantine window contains all of the actions that you can perform on Quarantined files.

Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on files that are already in Quarantine.
Properties	Provides detailed information about the selected file and the virus that is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.
Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect it.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus definitions for a while and then try to repair the files in Quarantine.

To perform an action on a file in Quarantine

1. Select the file on which you want to perform the action.
2. In the toolbar, select the action that you want to perform.
3. When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus cannot repair a file

See "Keeping current with LiveUpdate" on page 65.

One of the most common reasons that Norton AntiVirus Professional Edition cannot automatically repair or delete an infected file is that you do not have the most up-to-date virus protection. Update your virus protection with LiveUpdate and scan again.

If that does not work, read the information in the report window to identify the types of items that cannot be repaired, and then take the appropriate action.

File type	Action
Infected files with .exe, .doc, .dot, or .xls file name extensions (any file can be infected)	Use the Repair Wizard to solve the problem. See "Use the Repair Wizard" on page 74.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using the Rescue Disks or your operating system disks. See "About Rescue Disks" on page 40.

If your computer does not start properly

See "About Rescue Disks" on page 40.

If you have a virus on your computer and need to start the computer from an uninfected disk to remove the virus, or if you need to restore a *boot record*, use your Rescue Disks. If you do not have Rescue Disks, you can use your Emergency Disks to start the computer and remove the virus. If you need to restore boot records and do not have Rescue Disks, or if you need to restore system files, you must reinstall Windows.

If you need to use Rescue Disks (Windows 98/98SE/Me)

Sometimes a virus infection prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus Professional Edition alert tells you when to use your Rescue Disks.

You first need to determine if your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system
- Updated virus definitions

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk window appears, use only the Norton AntiVirus Professional Edition task.

To use your Rescue Disks

1. Insert the Basic Rescue Boot floppy disk into drive A and restart your computer.
   The Rescue program runs in DOS.
2. Use the arrow keys to select the program that you want to run.
   A description of the selected program appears in the right pane of the Rescue program. Your choices are:

Norton AntiVirus	Scans your computer for viruses and repairs any infected files
Rescue Recovery	Checks and restores boot and partition information

3. Press **Enter** to run the selected program.
4. Follow the on-screen instructions for inserting and removing the Rescue Disks.
5. When the Rescue program is done, remove the Rescue Disk from drive A and restart your computer.

If you need to use Emergency Disks

See "Create Emergency Disks" on page 26.

If you have not created Rescue Disks, you can use Emergency Disks to restart your computer and scan for viruses.

To use Emergency Disks

1. Insert Emergency Disk 1 into drive A and restart your computer.
   The Emergency program runs in DOS.
2. Ensure that Antivirus is selected, then press **Enter** to begin the Norton AntiVirus Emergency program.

3 Follow the on-screen instructions for inserting and removing the Emergency Disks.
The Emergency program automatically scans your computer and removes viruses.

4 When the Emergency program is done, remove the Emergency Disk from drive A and restart your computer.

If you are using the CD as an Emergency Disk

See "I cannot start from drive A" on page 96.

If you are using the Norton AntiVirus Professional Edition CD as an Emergency Disk, you can ignore all of the instructions to change disks, as all necessary information is on the CD.

You may need to change your computer's BIOS Setup options to start from the CD-ROM drive.

To use the CD as an Emergency Disk

1 Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.

2 Restart your computer.
The Emergency program scans your computer and removes viruses.

Look up viruses on the Symantec Web site

The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

1 Start Norton AntiVirus Professional Edition.

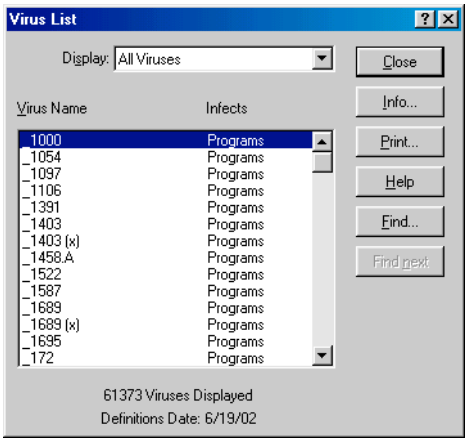
2 In the Norton AntiVirus Professional Edition main window, click **Reports**.

3 In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.
The Symantec Web site opens in your Internet browser.

4 Use the links on the Web page to access the virus information for which you are looking.

Look up viruses in Norton AntiVirus

If you don't have an active Internet connection, you can look up a virus name from within Norton AntiVirus Professional Edition. The Virus List dialog box lists the viruses in the current virus definition service files on your local computer. Because of the large number of viruses, the Virus List file does not include descriptions of each virus.



See "Keeping current with LiveUpdate" on page 65.

To ensure that you have the latest virus definitions, run LiveUpdate.

To look up virus names and definitions

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Reports**.
3. In the Reports pane, on the Virus List line, click **View Report**.

To get more information about a specific virus

1. In the Virus List dialog box, select the virus about which you want more information.
2. Click **Info**.
3. When you are done viewing the list, in the Virus List dialog box, click **Close**.

Recovering missing or erased files

7

If you purchased Norton AntiVirus Professional Edition to recover files, do not install Norton AntiVirus Professional Edition and do not start Windows. Any new files copied to your hard disk might overwrite existing data. Starting Windows writes to your hard disk. The Windows swap file could overwrite data you would like to recover. See "About Rescue Disks" on page 40.

About Norton Protection

When you erase a file using Windows Explorer, Windows keeps a temporary copy of the file in the Recycle Bin. However, Windows does not detect files that were erased or overwritten by applications running in Windows, erased from a command prompt, or deleted via a permanent method, such as using Shift+Delete.

The Norton Protected Recycle Bin protects the following types of files:

- Files that are deleted while you are using the command line
- Files created and deleted by Windows applications
- Older versions of files that you modify and overwrite
- Files that were deleted by viruses or other malicious threats, if they use a standard Windows or DOS deletion method
- If the standard Windows Recycle Bin is not enabled, Norton Protection also protects files that would otherwise be under Recycle Bin protection

Files shared on a network or stored on a network server and files deleted while using your computer in DOS mode rather than Windows are not protected.

To configure Norton Protection

1. On the Windows desktop, right-click the **Norton Protected Recycle Bin**, then click **Properties**.
2. On the Norton Protection tab, make sure that Enable Protection is checked.
3. On the Recycle Bin tab, select the item to open when the Recycle Bin icon is double-clicked.
   Use the context-sensitive Help to view more options in the Norton Protected Recycle Bin.

See "Use online Help" on page 52.

If you start your computer in DOS mode, you may find that DOS reports less free disk space than expected. This discrepancy is because DOS does not deduct the space used by deleted files protected by Norton Protection.

About UnErase Wizard

UnErase Wizard helps you recover deleted files from the Norton Protected Recycle Bin. In Windows 98/Me, UnErase Wizard can also help you restore files that were unprotected by Norton Protection. Windows 2000/XP can only recover files if Norton Protection is turned on.

UnErase Wizard also helps you recover files that are deleted from the standard Windows Recycle Bin. In Windows 98/Me, UnErase Wizard frequently recovers unprotected files as well, even those deleted from the Recycle Bin.

If you have a dual boot system and the volume containing deleted files is not NTFS, you can use the Windows 98/Me version of UnErase Wizard to recover deleted files.

Using UnErase Wizard, you can search for a deleted file by its file name and by words that you think the file may contain. This is especially useful if you can't remember the file name, but you do remember its contents.

Recover a file with UnErase Wizard

If you have excluded files from Norton Protection and these excluded files are deleted, they are not intercepted by the Windows Recycle Bin or Norton Protection and therefore are not recoverable on Windows 2000/XP systems.

UnErase Wizard displays a list of deleted files or the files that conform to file name criteria that you provide. Each file is described by its name, original location, the date it was deleted, *file type*, file size, and the program that was used to delete it. You can view the contents of a file before or after you recover it.

To recover a file with UnErase Wizard

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Advanced Tools**.
3. On the UnErase Wizard line, click **Start Tool**.
4. In the UnErase Wizard dialog box, select the action that you want to take. Your options are:

Find recently deleted files	Searches for the names of the most recently deleted files and displays up to a maximum of 25 deleted files (Windows 98/Me only).
Find all protected files on local drives	Searches for and displays the names of all deleted files that are protected by Norton Protection or the Windows Recycle Bin on your computer.
Find any recoverable files matching your criteria	Prompts you for search criteria. Use this option if you are looking for words that are contained in a deleted file.
Find all Norton Protected Users files	Searches for other users' protected files as well as your own. (This option is available only in Windows 2000/XP.)

5. Click **Next**.
   UnErase Wizard displays a list of the most recently deleted files.
6. Select the file that you want to recover.
7. Click **Recover**.
   If you want to examine the recovered file, make a note of the recovery destination.

8 If you are using Windows 98/Me and your deleted file is not listed, click **Next**.
UnErase Wizard guides you through the process of creating a more complete list of deleted files from which to select.

9 To close UnErase Wizard, click **Finish**.

If you delete a file on a floppy disk from a DOS prompt by specifying file name letters after a wildcard (such as DEL *ILENAME.TXT as opposed to DEL FILENAME.TXT or DEL *.TXT), the file is listed as unrecoverable on the Recently Deleted Files page.

To see if a file is recoverable

1 In the center of the file list, right-click, then click **Show Unrecoverable Files**.

2 Click **Next**.
Use the UnErase Wizard pages to search for and recover the files.

Eliminating data permanently

8

Wipe Info lets you remove selected files or folders from your hard disk.

If you are running a recovery application such as System Restore or GoBack 3 Personal Edition, you must erase your history before running Wipe Info to ensure that the data is completely wiped.

About Wipe Info

Wipe Info Wizard erases files or folders from your hard disk so that they cannot be recovered.

When you wipe a file, Wipe Info wipes the file and attempts to wipe any free space associated with the file and the file's directory entry.

When you wipe a folder, Wipe Info wipes all of the files in the folder, and then, if the folder is empty, it attempts to wipe the directory entry for the folder.

In general, you cannot recover files that have been wiped. Windows Me/XP System Restore can restore files that have been wiped if they are one of the protected file types. By default, many document types, such as .doc and .xls files in My Documents, are protected. Windows Me/XP System Restore maintains copies of protected files. Wiping the original file does not wipe the copy that Windows Me/XP System Restore maintains.

Wipe Info eliminates a file's contents from the disk, but does not remove the file name. While the file name remains on disk, it is no longer visible in Windows Explorer, and there is no data stored with it.

Never store sensitive information in a file name or attribute. This data can be replicated throughout your system without your knowledge, for example, in a list of most recently used files, or a file name search. This type of embedded information can be very difficult to remove from your computer.

About hexadecimal values

Wipe Info uses hexadecimal values to wipe files. Hexadecimal refers to the base 16 number system. This system is used by computer programmers to represent numbers in the binary number system, which uses the zero and one symbols in combinations to represent any number.

The hexadecimal system consists of the numbers 0 to 9 and the letters A to F, used in combinations. For example, the decimal number 14 is represented as the letter E in the hexadecimal system.

In Wipe Info options, you can specify values from 00 to FF, representing numbers from 0 to 255 respectively. You can type the value using a number or a character from A to F.

About the Government Wipe process

When you select Government Wipe, Wipe Info does the following:

- Overwrites the data with 00s
- Verifies the 00 overwrite
- Overwrites with FFs
- Verifies the FF overwrite
- Writes a random value, or a value that you choose from 00 to FF
- Verifies the random overwrite
- Reverifies the random overwrite to ensure that it was written correctly
- Repeats as many times as you specify, up to 100

Set Wipe Info options

You can specify how Wipe Info handles hidden, read-only, and system files. You can also specify the type of wipe to use. The following wiping methods are available:

Fast Wipe	Overwrites the data being wiped with the hexadecimal value of your choice.
Government Wipe	Combines several wiping and overwriting processes to conform to specifications in DoD (Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from digital media.

To change Wipe Info options

1. In the Norton AntiVirus Professional Edition main window, click **Advanced Tools**.
2. On the Wipe Info line, click **Start Tool**.
3. Click **Options**.
4. On the General tab, select the options for Read-only, System, and Hidden file types.
5. On the Wipe Type tab, select one of the following:
   - Fast Wipe
   - Government Wipe
6. In the Hex Value text box, type or specify the hexadecimal values that Wipe Info should use when it overwrites the wiped files space.
7. In the Times to Perform This Wipe text box, type the number of times that Wipe Info should repeat this process.
8. Click **Apply**.

Wipe files or folders

To wipe a file or folder in Windows 2000/XP, add it to the Wipe Info window.

To wipe files or folders in Windows 2000/XP

1. In the Norton AntiVirus Professional Edition main window, click **Advanced Tools**.
2. On the Wipe Info line, click **Start Tool**.
3. Click **Wipe Info**.
4. In the Wipe Info window, click **Browse**.
5. Select one of the following:
   - Folders
   - Files
6. Select the folder or file to wipe.
7. Click **Open**.
8. With the Wipe Info window open, locate a folder or file on your hard disk.
9. Drag the selected item into the Wipe Info file list.
10. Continue to drag all of the files and folders that you want to wipe into the Wipe Info list.
    If you add an item to the list by mistake, select the item, then click **Remove Item(s) from list**.
11. Click **Wipe All**.
12. Click **Yes** to confirm the warning.
    All of the files in the list are wiped.

Troubleshooting

9

The information in this chapter will help you solve the most frequently encountered problems. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site. You can find updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

Explore the Symantec service and support Web site

The Symantec service and support Web site offers information focused on your product and whether the product is for home or business use.

To explore the Symantec service and support Web site

1. Point your browser to www.symantec.com/techsupp
2. On the service and support Web page, click **I am a home/small business user**.
3. On the introduction Web page, in the column on the left, click a link for the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

1. On the left side of any Web page in the Symantec service and support Web site, click **search**.
2. Type a word or phrase that best represents the information for which you are looking.
   Use the following guidelines when searching the Symantec Web site:
   - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type install to find articles that include the word install, installation, installing, and so on.
   - Type multiple words to find all occurrences of any of the words. For example, type virus definitions to find articles that include virus or definitions or both.
   - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
   - Use a plus (+) sign in front of all of the search terms and a space between terms, if you use more than one term, to retrieve documents containing all of the words. For example, +Internet +Security finds articles containing both words.
   - For an exact match, type the search words in uppercase letters.
   - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, "purchase product", "MAC", "Norton SystemWorks" searches for all three phrases, and finds all articles that include any of these phrases.
3. Select the area of the Web site that you want to search.
4. Click **Search**.

Troubleshoot Norton AntiVirus Professional Edition problems

Here are some solutions to issues that might arise with Norton AntiVirus Professional Edition.

My Rescue Disk does not work

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type **A:RSHELL**, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one *operating system* installed, such as Windows 2000 and Windows 98.

To modify your Rescue Boot Disk

1. Start up from your hard drive.
2. Insert your Rescue Boot Disk into drive A.
3. At the DOS prompt, type **SYS A:**
4. Press **Enter**.
   This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

The alert tells me to use my Rescue Disks, but I did not create them

See "To create Emergency Disks" on page 27.

With your Norton AntiVirus Professional Edition CD you can create Emergency Disks. Although they are not as powerful as the Rescue Disks you create, you can use the Emergency Disks to recover from most common emergencies.

See "If you are using the CD as an Emergency Disk" on page 82.

You can use the CD that contains Norton AntiVirus Professional Edition as an Emergency Disk if your computer can start from the CD-ROM drive.

Once you have created the Emergency Disks, use them to solve the problem.

I cannot start from drive A

If your computer does not check drive A first on startup, use your computer's Setup program to change settings.

Be careful when making changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

1. Restart your computer.
   A message appears telling you the key or keys to press to run SETUP, such as Press <DEL> if you want to run SETUP.
2. Press the key or keys to launch the Setup program.
3. Set the Boot Sequence to boot drive A first and drive C second.
   Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your system, or contact your system's manufacturer.
4. Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

See "My Rescue Disk does not work" on page 95.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk.

Auto-Protect does not load when I start my computer

If the Norton AntiVirus Professional Edition Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

1. On the Windows taskbar, click **Start** > **Shut Down**.
2. In the Shut Down Windows dialog box, click **Restart**.
3. Click **OK**.

Norton AntiVirus Professional Edition may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under System, click **Auto-Protect**.
4. Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus Professional Edition may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under System, click **Auto-Protect**.
4. Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus Professional Edition is not configured to look.

To reset Norton AntiVirus Professional Edition scanning options

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under System, click **Manual Scan**.
4. Under Which file types to scan for viruses, click **Comprehensive file scanning**.
5. Click **Manual Scan** > **Bloodhound**.
6. Ensure that Enable Bloodhound heuristics is checked, and click **Highest level of protection**.
7. Click **OK**.
8. Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

See "If you need to use Rescue Disks (Windows 98/98SE/Me)" on page 80.

Another reason could be that the virus is remaining in memory after you remove it from the *boot record*. It then reinfects your boot record. Use your Rescue Disks to remove the virus.

If the problem is a Trojan horse or worm that was transmitted over a shared *network* drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus Professional Edition delete the problem.

Norton AntiVirus Professional Edition cannot repair my infected files

See "Keeping current with LiveUpdate" on page 65.

The most common reason that Norton AntiVirus Professional Edition cannot repair your *infected files* is that you do not have the most current virus protection on your computer. Update your virus protection regularly to protect your computer from the latest viruses.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

See "If you have files in Quarantine" on page 78.

- Quarantine the file and submit it to Symantec.
- If a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I get an error when testing basic Rescue Disks

If you get the message Non-system disk, replace the disk and press any key when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

1. Remove the Rescue Boot Disk and restart your computer.
2. Insert the Rescue Boot Disk into the floppy disk drive.
3. On the Windows taskbar, click **Start** > **Run**.
4. In the Run dialog box, type **SYS A:**
5. Click **OK**.

I can't receive email messages

There are three possible solutions to this problem.

Temporarily disable email protection. This might allow the problem email message to download so that you can once again enable email protection. You are protected by Auto-Protect and Script Blocking while email protection is disabled.

To temporarily disable incoming email protection

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under Internet, click **Email**.
4. Uncheck **Scan incoming Email**.
5. Click **OK**.
6. Download your email messages.
7. Reenable incoming email protection.

See "About Internet options" on page 47.

Your email client may have timed out. Make sure *timeout* protection is enabled.

If you continue to experience problems downloading email messages, disable email protection.

To disable email protection

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under Internet, click **Email**.
4. Uncheck **Scan incoming Email**.
5. Uncheck **Scan outgoing Email**.
6. Click **OK**.

I can't send email messages

If you get the message, Norton AntiVirus Professional Edition was unable to send your email message because the connection to your email server was disconnected, your email client may be set to automatically disconnect after sending and receiving mail.

For Norton AntiVirus Professional Edition to scan outgoing email messages for viruses, it intercepts and scans the messages before they are sent to your email provider. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this, or disable Norton AntiVirus Professional Edition outgoing email scanning.

To disable outgoing email scanning

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Options**.
3. In the Options window, under Internet, click **Email**.
4. Uncheck **Scan outgoing Email**.
5. Click **OK**.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- PriorityCare telephone support
  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12 andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 25, 2002

Glossary

access rights	The types of operations and files a user or group can access and what the user or group is permitted to do with those directories and files.
administrator	1. A person who oversees the operation of a network. 2. A person responsible for installing programs on a network and configuring them for distribution to workstations. This person may also update security settings on workstations.
alert	A dialog box that appears in a graphical user interface (GUI) to signal that an error has occurred, or to provide a warning.
beam	To transfer data by infrared transmission.
boot record	A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot record also contains a program that loads the operating system.
browser	A software application that makes navigating the Internet easy by providing a graphical user interface. This lets the user click menus, icons, or buttons rather than learn difficult computer commands. Also called a Web client.

compressed file	A file that has been compressed using a special data storage format in order to save space on your disk.
compression	Using a mathematical algorithm to process data from a file or disk, such that the resulting data occupies less physical space on the disk. Individual files or entire disks can be compressed by various types of utility software.
disk icon	An icon representing a disk.
document file	A file that is created by, or associated with, a program and contains no executable code. Examples include word processing documents, databases, and spreadsheets.
download	To transfer a file from one computer system to another, through a modem or network. Download usually refers to the act of transferring a file from the Internet, a BBS (bulletin board system), or a service such as America Online.
download directory	The directory in which files received during file transfer are stored.
email (electronic mail)	A method of exchanging messages and files with other people via computer networks. A popular protocol for sending email is SMTP (Simple Mail Transfer Protocol). Popular protocols for receiving email are POP3 (Post Office Protocol 3) and IMAP4 (Internet Message Access Protocol 4). Web-based email services use HTTP (Hypertext Transfer Protocol) for sending and receiving email.
executable file	A file containing program code that can be launched. Generally includes any file that is a program, extension, or a system file.
file server	A storage device connected to a network that provides network users access to shared programs and data files.

file type	A code that is stored in each file that associates it with a program or activity.
hard disk	A device that reads data from, and writes data onto, a disk.
HTML (Hypertext Markup Language)	A standard language for documents on the World Wide Web. Codes inserted in a text file instruct the Web browser on how to display a Web page's words and images for the user, and define hypertext links between documents.
icon	A graphic symbol used to represent a file, folder, disk, or other entity.
infected file	A file that contains a virus, Trojan horse, or worm.
Internet	A decentralized global network connecting millions of computers.
known virus	A virus for which Norton AntiVirus Professional Edition has a definition. See also virus definition.
LAN (Local Area Network)	A group of computers connected for the purpose of sharing resources. The computers on a local area network are typically located within a defined physical space, such as a single building, or section of a building.
local	A term that refers to your computer, as opposed to a remote computer.
locked disk	See write-protect.
locked file	A file that can be viewed, but cannot be written to or deleted. Also referred to as read-only.
log	A record of actions and events that take place on a computer.

network	A set of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware among users.
newsgroups	A discussion forum on the Internet that provides articles and posting opportunities for its members. A newsgroup is typically focused on a particular subject or range of subjects.
operating system	A program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mouse devices.
password	A character sequence entered by users to verify their identities to a network or program. The most secure passwords are difficult to guess or find in a dictionary, and contain a combination of capital letters, lowercase letters, numbers, and symbols.
POP3 (Post Office Protocol 3)	An email protocol used to retrieve email from a remote server over an Internet connection.
program	A set of instructions that can be executed by a computer, and are written for a specific purpose such as word processing or creating a spreadsheet. Also called software.
Quarantine	A disk location established by Norton AntiVirus to isolate files suspected to contain a virus so that the files can't be opened or executed.
read-only	A disk, folder, or file containing data that can be read, but cannot be written to or deleted. Also referred to as locked or write-protected.

removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, disk cartridges (such as SyQuest and Bernoulli, for example), CDs, and Zip disks.
script	A list of instructions that can be executed without user interaction. Unlike other types of programs, scripts can be opened with text editors or word processing programs, so they are very easy to change. Examples of scripts include Visual Basic programs and network login scripts.
startup disk	A disk that contains the system files necessary to start your computer. Startup disk usually refers to a floppy disk or CD that can be used to start the computer in an emergency.
threat	A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.
timeout	A predetermined period of time during which a given task must be completed. If the timeout value is reached before or during the execution of a task, the task is canceled.
Trojan horse	A destructive program often designed to cause damage or do something malicious to a system, while disguised as something useful or interesting. Unlike viruses, Trojan horses don't make copies of themselves. Some Trojan horse programs perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote-control capabilities for hackers.
unknown virus	A virus for which Norton AntiVirus Professional Edition does not contain a definition. See also virus definitions file.

virus	A self-replicating program intentionally written to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display annoying messages. Self-replication differentiates viruses from other virus-like computer infections such as Trojan horse programs and worms. See also virus-like activity.
virus definition	Virus information that lets an antivirus program recognize and alert you to the presence of a specific virus. See also unknown virus.
virus definitions file	A file used by Norton AntiVirus to find and repair viruses. The virus definitions files must be updated regularly. LiveUpdate automates the process of downloading updated virus definitions files.
Virus List	A list that shows all of the viruses for which Norton AntiVirus has a virus definition. It is important to update this list regularly.
virus-like activity	An activity or action that Norton AntiVirus Professional Edition perceives as the work of a possible unknown virus. Virus-like activity alerts do not necessarily indicate the presence of a virus, but should be investigated.
Web page	A single document on the World Wide Web that is identified by a unique URL. A Web page can contain text, hyperlinks, and graphics.
Web site	A group of Web pages managed by a single company, organization, or individual. A Web site may include text, graphics, audio and video files, and hyperlinks to other Web pages.

World Wide Web	The collection of hypertext documents that are stored on Web servers around the world. Also called WWW or simply the Web. The Web allows universal access to a vast collection of documents stored in HTML format as Web pages.
worm	A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down. So far, worms do not exist in the Macintosh world.
write-protect	Write-protecting disks prevents viruses from infecting them. To write-protect a 3.5-inch disk, slide the tab on the back of the disk to uncover the hole through the disk. Also referred to as a locked disk or read-only disk.

Index

A

accessing
  UnErase Wizard 87
accessing Options 44
Activity Log 16, 50
Adobe Acrobat Reader, installing 53
AOL 68
Automatic LiveUpdate 47, 70
Auto-Protect
  description 39
  disabling 39
  enabling 40, 57
  failure to load on startup 97
  options 46

B

backing up file before repair 48
Bloodhound
  options 46
  technology 19
booting
  absent 95
  Auto-Protect failure to load 97
  changing floppy disk drive settings 96
  floppy disk drive fails 96
  Rescue Disk fails 95

C

CD-ROM drive, starting Norton AntiVirus from 82
changing scan schedules 64
changing settings 44
checking for recoverable files 88
CompuServe 68
computer requirements 23
connecting to the Internet automatically 70
Contents tab in Help 52
context-sensitive Help 52
creating
  Emergency Disks 26
  Rescue Disks 41
custom scans
  changing schedule 64
  deleting 62
  deleting schedule 64
  running 61
  scheduling 62

D

default options 49
definitions of technical terms 51
deleting
  custom scans 62
  infected files 75
  scan schedule 64
dialog box Help 52
Disabling

Automatic LiveUpdate 71
Auto-Protect 39
displaying the Norton AntiVirus toolbar 38

E

electronic newsletter 56
eliminating data permanently 89
Emergency Disks
creating 26
using 81
using the CD 82
emergency preparations 22
enabling
Automatic LiveUpdate 47
Auto-Protect 40
Office Plug-in 48

F

file extensions, unusual 98
file scans 59
files
check if recoverable 88
security considerations 90
files, reinfected after virus removal 98
firewalls, using LiveUpdate 67
floppy disk scans 59
floppy drives, unable to boot from 96
folder scans 59
full system scans 59

G

glossary 51
GoBack and Wipe Info 89

H

hard drive scans 59
Help
context-sensitive 52
in dialog boxes 52
online Help 52
procedural 52
hexadecimal values in Wipe Info 90

I

Index tab in Help 52
infected files
cannot repair 98
reinfected 98
Information Wizard
features 32
how to use 32
when it appears 31
Inoculation
alerts 78
options 48
responding to alerts 78
instant messenger
options 47
scanning files 16
scanning transferred files 57
Internet options 47
Intrusion Detection service 66

J

JavaScript scripts 19

L

launching Norton AntiVirus Professional Edition 37
list of viruses 18
LiveUpdate options 47
Log Viewer 16
activities in 50
contents 50
monitoring activities in 50

M

macro viruses 17
macros, defined 17
Miscellaneous options 48
multiple schedules for a scan 63

N

networks, using LiveUpdate 67
new features in Norton AntiVirus Professional Edition 15
newsletters 56
Norton AntiVirus
  updating virus definitions 68
  Windows tray icon 39
Norton AntiVirus Professional Edition
  accessing from Windows Explorer 38
  starting 37
  tools 37

O

Office Plug-in
  enabling 48
  status 44
online Help 52
online tutorials 55
online Virus Encyclopedia 54, 82
operating systems 23
operating systems, multiple 95
Options
  accessing 44
  Auto-Protect 46
    Advanced 46
    Bloodhound 46
    Exclusions 46
  changing settings 48
  email
    Advanced 47
    scanning 47
  Inoculation 48
  instant messenger 47
  Internet 47
  LiveUpdate 47
Options (*continued*)
  Manual Scan 46
    Bloodhound 46
    Exclusions 46
  Miscellaneous 48
  Other 48
  resetting defaults 49
  Script Blocking 46
  settings categories 45
  Wipe Info 91
Other options 48

P

password protection
  option 16, 48
Prodigy Internet connection 68
product serial number 32

Q

Quarantine
  files in 78
  infected files in 75
  options 79

R

registering your software 32
removable drive scans 59
removing
  other antivirus programs 25
  previous copies of Norton AntiVirus 25
removing Norton AntiVirus Professional Edition from your computer 35
repairing infected files
  in Windows 2000/XP 76
  in Windows 98/98SE/Me 75
required computer configuration 23
Rescue Disks
  absent 95
  creating 41
  defined 40
  failure to start from 95
  testing 41
  updating 42
  using 80, 81

restoring boot record and system files 80
running custom scans 61

S

safe mode 97
scan files at startup 48
Scan Summary 74
scanning
  automatic 62
  during installation 27
  entire computer 59
  from a boot disk 80
  individual elements 59
scheduling
  custom scans 62
  LiveUpdate 70
  virus scans 62
Script Blocking 19
  monitoring by 57
  virus found by 77
security response Web page 55
serial number 32
Service and Support 101
setting options 44
settings categories 45
setup program, changing boot drive sequence 96
starting
  Norton AntiVirus from the CD-ROM drive 82
  Norton AntiVirus Professional Edition 37
  your computer from a floppy disk 80
startup
  Auto-Protect failure to load 97
  changing floppy disk drive settings 96
  floppy disk drive fails 96
  Rescue Disk fails 95
  Rescue Disks absent 95
  scan files at 48
startup alert about virus protection 48
submitting files to Symantec 79
subscriptions 66
Symantec Response Center Web site 54
Symantec Security Response newsletter 56
Symantec service and support Web site 93
Symantec Solutions Web site 54
Symantec Store Web site 54
Symantec Web site 54, 55, 82
  connecting 38
  downloading product updates 68
system status 43

T

Technical Support 101
Technical Support Web site 54
testing Rescue Disks 41
tray icon 39
Trojan horses 17
troubleshooting 95
tutorials 55

U

UnErase Wizard
  accessing 87
  features 86
uninstalling
  Norton AntiVirus Professional Edition 35
  other antivirus programs 25, 26
  previous copies of Norton AntiVirus 25
updating
  from Symantec Web site 68
  Rescue Disks 42
  virus protection 68
User's Guide PDF 53, 54

V

version number, checking 39
viewing the Activity Log 50
virus alert options 75
virus definition service 18
virus definitions 18
  alternate sources 68
  described 66
  downloading from Symantec Web site 68
  updating with LiveUpdate 68
virus descriptions 18
virus encyclopedia 55

Virus List 83
virus protection
  alerts 48
  system scans 59
  updating 70
virus repair
  in Windows 2000/XP 76
  in Windows 98/98SE/Me 75
viruses
  before you install 25
  behavior 18
  defined 16
  found by Auto-Protect 75
  found during a scan 73
  looking up in Norton AntiVirus Professional Edition 83
  looking up on Symantec Web site 82
  submitting to Symantec 79
  viewing descriptions 82
Visual Basic scripts 19

W

Web filtering service 66
Web sites, Symantec 68
Windows 2000, Wipe Info procedure 92
Windows Explorer menu, displaying 38
Windows operating systems 23
Windows safe mode 97
Windows tray icon 39, 40
Windows XP
  System Restore after Wipe Info 89
  Wipe Info procedure 92
Wipe Info 89
  and GoBack 89
  and Windows Me/XP System Restore 89
  characters used to wipe 90
  Government Wipe 90
  options 91
  procedure on Windows 2000/XP 92
wizards
  UnErase Wizard 86
  Wipe Info Wizard 89
Worm Blocking
  introducing 16
  monitoring by 57
  threats found by 77
worms 17

Norton AntiVirus™ Professional Edition

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

If your Symantec product was installed on your computer when you purchased it, contact your hardware manufacturer for CD replacement information.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please) _____

City _____ State _____ Zip/Postal Code _____

Country* _____ Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: _____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	
Shipping & Handling	$ 9.95
TOTAL DUE	

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%).
Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _____ __ Visa __ Mastercard __ AMEX

Credit Card Number _____ Expires _____

Name on Card (please print) _____ Signature _____

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

Symantec and Norton AntiVirus are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2002 Symantec Corporation. All rights reserved. Printed in the U.S.A.

symantec™